

EXHIBIT 3

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE
COMMISSION,

Plaintiff,

v.

SOLARWINDS CORP. and TIMOTHY G.
BROWN,

Defendants.

Civil Action No. 23-cv-9518-PAE

**EXPERT REPORT OF MARK G. GRAFF
OCTOBER 25, 2024**

TABLE OF CONTENTS

I.	INTRODUCTION AND QUALIFICATIONS	1
A.	Qualifications.....	1
B.	Relevant Parties and Summary of Allegations	4
1.	Relevant Parties	4
2.	Summary of Allegations	5
C.	Assignment	6
D.	Facts and Data Considered.....	7
II.	SUMMARY OF OPINIONS	8
III.	FACTUAL BACKGROUND.....	13
A.	General Background on Cybersecurity and the Cybersecurity Practices of Corporations	13
B.	Background on SolarWinds	17
IV.	ANALYSIS AND OPINIONS	20
A.	Research Methodology and Analytical Framework	20
B.	SolarWinds Internal Documentation and Testimony Show That SolarWinds Did Not Consistently Follow the Assertions in the Security Statement Regarding Access Controls	25
1.	Introduction to access control	26
2.	The SolarWinds Security Statement made assertions about access control.....	28
3.	SolarWinds failed to follow access control practices asserted in the Security Statement	29
C.	SolarWinds Internal Documentation and Testimony Show That SolarWinds Did Not Consistently Follow the Assertions in the Security Statement Regarding Passwords and User Authentication.....	62
1.	Introduction to passwords and user authentication.....	63
2.	The SolarWinds Security Statement made assertions about passwords and user authentication.....	64
3.	SolarWinds failed to follow the password and user authentication practices asserted in the Security Statement	64
D.	SolarWinds' Internal Documentation and Testimony Show That, Contrary to the Security Statement, SolarWinds Did Not Consistently Follow "Standard Security Practices" in Its Secure Development Lifecycle	75
1.	Introduction to secure development lifecycle and security testing.....	76

2. The SolarWinds Security Statement made assertions about
a secure development lifecycle and security testing 81

3. SolarWinds failed to follow the SDL and security testing
procedures as asserted in the Security Statement 82

I. INTRODUCTION AND QUALIFICATIONS

A. Qualifications

1. My name is Mark G. Graff. I have over 40 years of experience as a computer programmer, technologist, and cybersecurity executive. Additionally, I have designed cyber defenses, managed the groups that operated those defenses, written security plans and security policies, and overseen the response to many cybersecurity incidents. These days I operate a cybersecurity consulting company, Tellagraff LLC, a company I founded in 2014, working as a consultant to industry and government, as an expert witness, and as a university lecturer.

2. As a consultant, I work with both government and private businesses to evaluate and remediate cybersecurity threats and risks, and also provide guidance on technical product development, including the use of secure development practices. I have been interviewed as a cyber expert for national news outlets and publications including CNN International, CBS News, and The Wall Street Journal, and have testified before Congress twice. I hold a B.S. in Computer Science from the University of Southern Mississippi.

3. Previously, I served as the Chief Information Security Officer (“CISO”) of NASDAQ OMX and as the Chief Cyber Security Officer at Lawrence Livermore National Laboratory (“LLNL”). At NASDAQ, I led a team of software developers and other specialists to secure NASDAQ’s worldwide operations against cyber-attacks by foreign countries, criminal organizations, and other hostile entities. I also directed NASDAQ’s global security policy, implemented employee cybersecurity awareness and training, and developed secure software applications, among other responsibilities. At LLNL, I managed the organization’s Cyber Security Program, including incident response activities, employee security training, and internal

audits for classified and unclassified systems. I conducted numerous cybersecurity research projects and risk analyses, some classified, in the interest of national security. I also served as an advisor to the senior executive team of the Laboratory on cyber policy and strategy.

4. Prior to my roles at NASDAQ and LLNL, I spent twenty years in various cybersecurity roles at Sun Microsystems, Para-Protect Services, and as a private practice technology consultant with an emphasis on information security. At Para-Protect Services, I helped develop the incident prevention and response unit of the firm's managed security service portfolio, including conducting security trend and threat analysis. At Sun Microsystems, I worked in several roles, including Global Network Security Architect. My responsibilities included managing the overall security of the Sun Wide Area Network as well as coordinating the evaluation of security risks and issues of key application software that Sun Microsystems used to run its worldwide enterprises, in approximately 130 countries. I also served as Chairman of the Forum of Incident Response and Security Teams ("FIRST"), an international association of enterprise cyber-defense teams.

5. Currently, in addition to my consulting work, I am an adjunct professor of Computer Science at the University of Arkansas Little Rock. I have taught two courses there, "Software Security" (CSEC 3322) and "System Security" (CSEC 2310). CSEC 3322 addresses Software Development Lifecycle methods designed to produce software that is as secure against attackers as possible. One of my books ("Enterprise Security Software", see below) is the textbook for this class. The other course, CSEC 2310, teaches a comprehensive approach to securing a computer – or a network – by making a sound security plan; selecting appropriate defensive methods (e.g., sound access controls); monitoring events; and responding to incidents.

In teaching this latter course I cover in detail NIST guidelines and resources such as the Cybersecurity Framework and Special Publication 800-53.¹

6. I have also co-authored three books on the subject of security and software. My book *Secure Coding: Principles and Practices* was one of the earliest books to address how to develop, test, and deploy software that is difficult to successfully attack.² This book has been used at dozens of universities to teach how to design and build secure software-based systems.³ In *Enterprise Software Security: A Confluence of Disciplines*, my co-authors and I described a holistic approach to bring software engineering and network security teams together to develop secure software using widely-accepted techniques.⁴ I also wrote the chapter on “Identity and Access Management” (in other words, user authentication and access control) in the book “The Official (ISC) Guide to the CISSP CBK Reference.”⁵

7. I have testified before Congress on matters of Internet and software security; served as an expert witness in lawsuits relating to software security and consumer safety; and consulted as an expert in cybersecurity for California in matters regarding election security. I have also appeared before the Presidential Commission on Infrastructure Survivability and the

¹ As I describe in Section III.A, the National Institute of Standards and Technology (NIST) “develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies and the broader public.” NIST, “Cybersecurity,” <https://www.nist.gov/cybersecurity>.

² Graff, Mark G. and Kenneth R. Van Wyk, “Secure Coding: Principles and Practices,” O’Reilly Media, June 30, 2003 (“Graff and Van Wyk (2003) Secure Coding: Principles and Practices”).

³ This book describes in detail each stage of the secure software development lifecycle, which I will discuss in **Section IV.D** of my expert report.

⁴ Van Wyk, Kenneth R., Mark G. Graff, Dan S. Peters, et al., *Enterprise Software Security: A Confluence of Disciplines*, Addison Wesley Professional, December 7, 2014.

⁵ John, Warsinske, Mark Graff, Kevin Henry, et al., “Chapter 5 - Identity and Access Management,” *The Official (ISC) Guide to the CISSP CBK Reference*, 5th Ed., Wiley, April 2019 (“Warsinske et al. (2019) Chapter 5 - Identity and Access Management”).

Securities and Exchange Commission (“SEC”) to offer my opinions on cybersecurity challenges and priorities.

8. A copy of my CV is attached as **Appendix A** to this expert report. A list of the trial and deposition testimony that I have offered in the last five years is attached as **Appendix B** to this report.

B. Relevant Parties and Summary of Allegations

1. Relevant Parties

9. SolarWinds Corporation (“SolarWinds”) offers software solutions that allow its customers to observe, monitor, and manage the performance of their information technology (“IT”) environments.⁶ After its founding in 1999, SolarWinds conducted its first initial public offering (“IPO”) in 2009,⁷ before being acquired and taken private by private equity firms in 2016.⁸ Then, on October 18, 2018, SolarWinds conducted a second IPO, and it has since been traded under the ticker symbol “SWI.”⁹

10. Timothy G. Brown joined SolarWinds in 2017 as Vice President of Security, and his role expanded to CISO in 2021.¹⁰ According to a SolarWinds press release from May 2021,

⁶ SolarWinds, “Corporate Overview,” *available on* April 30, 2019, <http://web.archive.org/web/20190430082154/https://investors.solarwinds.com/overview/default.aspx>.

⁷ Baker, Liana B. and Greg Roumeliotis, “SolarWinds Confirms It Is Exploring Strategic Alternatives,” Reuters, October 9, 2015, <https://www.reuters.com/article/us-solarwinds-m-a/exclusive-solarwinds-in-talks-with-buyout-firms-about-a-sale-sources-idUSKCN0S31OT20151009>.

⁸ Assis, Claudia, “Software Provider SolarWinds Files for IPO,” MarketWatch, September 21, 2018, <https://www.marketwatch.com/story/software-provider-solarwinds-files-for-ipo-2018-09-21>.

⁹ SolarWinds Corporation, SEC Form S-1, filed October 18, 2018, pp. 12, 41.

¹⁰ Deposition of Timothy Brown, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, October 3, 2024 (“Brown Deposition”) at 21:16-22:4, 25:9-13; Investigative Testimony of Timothy Brown - Vol. I, March 8, 2022 (“Brown Investigative Testimony, Vol. I”) at 13:19-14:18.

Mr. Brown’s responsibilities include “internal IT security, product security and security strategy,” as well as SolarWinds’ “security compliance, internal audit, IT operations, risk measurement and remediation efforts.”¹¹ The press release also stated that Mr. Brown’s over 25-year experience “developing and implementing security technology,” including patented technology related to security, allows him to “understand[] the challenges and aspirations of the person responsible for driving digital innovation and change.”¹²

2. *Summary of Allegations*

11. The SEC filed its complaint against SolarWinds and Mr. Brown on October 30, 2023, which it amended on February 16, 2024 (the “Amended Complaint”).¹³

12. I understand from the Amended Complaint that the SEC alleges that, at least between October 2018 and January 12, 2021 (the “Relevant Period”), “SolarWinds and/or Mr. Brown made materially false and misleading statements and omissions related to SolarWinds’ cybersecurity risks and practices” in SolarWinds’ public disclosures.¹⁴

13. Specifically, the SEC alleges SolarWinds and Mr. Brown concealed from the public that, throughout the Relevant Period, SolarWinds:

¹¹ SolarWinds, “SolarWinds Accelerates Its Plan for a Safer SolarWinds and Customer Community with the Appointment of Three New Executives,” May 4, 2021, <https://investors.solarwinds.com/news/news-details/2021/SolarWinds-Accelerates-its-Plan-for-a-Safer-SolarWinds-and-Customer-Community-With-the-Appointment-of-Three-New-Executives/default.aspx>.

¹² SolarWinds, “SolarWinds Accelerates Its Plan for a Safer SolarWinds and Customer Community with the Appointment of Three New Executives,” May 4, 2021, <https://investors.solarwinds.com/news/news-details/2021/SolarWinds-Accelerates-its-Plan-for-a-Safer-SolarWinds-and-Customer-Community-With-the-Appointment-of-Three-New-Executives/default.aspx>.

¹³ Amended Complaint, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, February 16, 2024 (“Amended Complaint”).

¹⁴ Amended Complaint ¶ 6.

- a. failed to “remedy access control problems;”
- b. failed to “enforce the use of strong passwords on all systems;”
- c. failed to adhere to the steps of the secure development lifecycle that it publicly claimed to follow;
- d. failed to “adequately monitor its networks;”¹⁵ and
- e. failed to comply with many aspects of the National Institute of Standards and Technology (“NIST”) Cybersecurity Framework to which it publicly claimed to adhere.¹⁶

14. According to the Amended Complaint, SolarWinds and Mr. Brown made these statements throughout the Relevant Period in its “Security Statement,” which SolarWinds posted on its website and/or sent to its customers, claiming to describe SolarWinds’ cybersecurity practices and policies.¹⁷

C. Assignment

15. I have been retained on behalf of the Plaintiff as an independent expert in connection with the matter of *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*.¹⁸

16. My hourly rate for work on this matter is \$1,000. Some of the work underlying the conclusions of my expert report was performed under my direction and guidance by

¹⁵ Amended Complaint ¶ 8.

¹⁶ Amended Complaint ¶ 72.

¹⁷ Amended Complaint ¶¶ 6, 57.

¹⁸ Amended Complaint.

employees at Analysis Group, Inc., an economic and litigation consulting firm. Neither my compensation nor that of Analysis Group, Inc., is contingent upon my findings, the testimony I may give, or the outcome of this litigation.

17. I have been retained to provide my analysis and opinions on a technical comparison between (1) the state of cybersecurity depicted in the Security Statement posted on its public website between 2017 and 2020 and (2) SolarWinds' internal assessments, presentations, and communications regarding the state of cybersecurity during that same timeframe with respect to the areas described below:

- a. Methods for access control;
- b. Methods for user authentication;
- c. Use of a secure development lifecycle;
- d. Methods for network monitoring; and
- e. Adherence to the NIST Cybersecurity Framework.

D. Facts and Data Considered

18. In forming my opinions, I have reviewed documents and other materials provided to me by counsel for the SEC or obtained from public sources. These materials include, among others, depositions and associated exhibits; internal SolarWinds communications, presentations, and analyses; and SolarWinds public disclosures during or around the Relevant Period.¹⁹ The

¹⁹ As of the date of this report, I have been provided the rough transcripts for the depositions of Jason Bliss and Ian Thornton-Trump, but not the final transcripts. Once I receive the final transcripts, I will review them and, if anything is different from the rough transcripts, may update my report.

sources that I considered are identified in this report and the accompanying exhibits are listed in the attached **Appendix C**.

19. Should additional relevant documents or information be made available to me, I reserve the right to update, refine, or supplement my opinions, or form additional opinions, as appropriate.

II. SUMMARY OF OPINIONS

20. Based on my experience in evaluating the cybersecurity practices of large organizations, my review of SolarWinds' internal documentation, communications, and testimony, and considering the language of the SolarWinds Security Statement, I conclude that the state of cybersecurity depicted in SolarWinds' internal discussions did not match several of the very broad, categorical and unqualified assertions in the Security Statement.

21. I first note that some of the assertions in the Security Statement were too vague for me to evaluate. For example, the assertion that "SolarWinds follows the NIST Cybersecurity Framework with layered security controls to help identify, prevent, detect, and respond to security incidents" is a vague statement.²⁰ The NIST Cybersecurity Framework ("CSF") is not literally a standard. The goal of the NIST CSF is to "help an organization to align and prioritize its cybersecurity activities with its business / mission requirements, risk tolerances, and resources."²¹ That is, the NIST CSF presents a menu of recommended security controls reflecting well-accepted cybersecurity norms, but does not prescribe which of the controls the

²⁰ SW-SEC00466120–142 (SolarWinds' Security Statement) at 129.

²¹ NIST, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, April 16, 2018 ("NIST Cybersecurity Framework"), p. v.

organization must adopt.²² Therefore, an assertion that an organization “follows” the NIST CSF is not verifiable because, while one can—and I have—evaluated the extent to which an organization implements the recommended controls, there is, in the CSF, no requirement of which specific controls must be adopted.^{23,24} However, this specific reference that “SolarWinds follows the NIST Cybersecurity Framework,” to me indicates that SolarWinds routinely followed cybersecurity norms and best practices. In this report, I show that this was not the case.

22. Because I consider the assertion that “SolarWinds follows the NIST Cybersecurity Framework” not to be verifiable or falsifiable, I did not undertake a separate analysis regarding SolarWinds’ adherence to the NIST Cybersecurity Framework. Instead, I considered whether SolarWinds followed cybersecurity norms and best practices in my analysis of the other four areas in my assignment: (1) methods for access controls; (2) methods for user authentication; (3) use of a secure development lifecycle process; and (4) methods for network monitoring.

23. My main conclusion is that many of the cybersecurity practices discussed in internal SolarWinds documents were inconsistent, from a cybersecurity perspective, with the Security Statement’s representations regarding, at least, three of the four main areas of focus in my assignment. Specifically, in my opinion, with respect to access control, user authentication, and secure development lifecycle processes, there were significant discrepancies between the

²² NIST also provides advice in relation to documentation about which controls the organization should consider applying based on its evaluation of its risks. *See* NIST Cybersecurity Framework, pp. 24-44.

²³ In my statement that certain phrases or sentences are “not verifiable,” I mean this from a cybersecurity perspective. I am not offering a legal opinion as to whether they could be a materially misleading statement.

²⁴ NIST does have recommendations on how organizations should decide which controls to adopt. *See* NIST Cybersecurity Framework, p. 22. (“The Framework Core presented in this appendix represents a common set of activities for managing cybersecurity risk. While the Framework is not exhaustive, it is extensible, allowing organizations, sectors, and other entities to use Subcategories and Informative References that are cost-effective and efficient and that enable them to manage their cybersecurity risk.”).

cybersecurity practices SolarWinds claimed to be performing and the cybersecurity practices I have observed from its internal documents. Internal SolarWinds documents additionally indicate that significant deficiencies within these three areas were known or made known to the relevant cybersecurity and leadership personnel.²⁵

24. While I do not offer a similar opinion regarding SolarWinds' network monitoring practices, this does not mean that the assertions in the Security Statement related to network monitoring were accurate. Rather, within the documents that I have reviewed, I found insufficient evidence either to evaluate SolarWinds' network monitoring practices or to evaluate whether SolarWinds personnel were aware of any deficiencies in this area or discordances with the related assertions in the Security Statement.

25. However, many internal documents related to access control, user authentication, and secure development lifecycle processes indicate that relevant cybersecurity and leadership personnel were aware of SolarWinds' failure to consistently follow the widely accepted industry norms to which the Security Statement asserted that SolarWinds adhered in these three areas. My decades of experience have taught me that no organization has perfect cybersecurity and that any organization diligently assessing its cybersecurity will uncover, from time to time, some issues needing to be addressed. However, the cybersecurity problems that I explain in this expert report, reflected in the SolarWinds internal documents and testimony, do not constitute the kind of routine minor problems that a company would encounter if it followed security best practices and industry norms in the manner described in the Security Statement.²⁶ In my opinion, the

²⁵ By "relevant cybersecurity and leadership personnel" at SolarWinds, I refer to the SolarWinds employees described in **Table 1** below.

²⁶ I note that my conclusion contrasts with SolarWinds' assertion in its Memorandum of Law in Support of Defendants' Motion to Dismiss the Amended Complaint: "At most, the alleged facts indicate that SolarWinds

discrepancies between SolarWinds’ internal documents and Security Statement within the areas of access control, user authentication, and secure development lifecycle processes are reflective of significant deviations from industry norms, with potential company-wide impact, and in some cases an impact on the security of its customers as well.

26. On the basis of my review of the information identified herein, I have reached the following opinions:

- a. The practices SolarWinds described in internal documents were inconsistent, from a cybersecurity perspective, with certain **access control** related assertions made in the Security Statement. SolarWinds did not consistently, in the manner that was represented in the Security Statement, (1) set access controls based on a need-to-know or least privilege basis; (2) limit employees’ access to those resources that were required to perform their roles; or (3) revoke the access of those employees who left the organization.
- b. The practices SolarWinds described in internal documents were inconsistent, from a cybersecurity perspective, with certain **user authentication** related assertions made in the Security Statement. SolarWinds did not, in the manner that was represented in the Security Statement, enforce the use of unique account IDs. In addition, the Security Statement asserts that SolarWinds had “password best practices,” which I understand to be a reference to industry norms. Despite this, I found several instances in which SolarWinds violated industry norms related to

identified gaps in its policies from time to time for purposes of continually improving its cybersecurity posture—which is fully consistent with the Security Statement and with what reasonable investors would expect.”
 Memorandum of Law in Support of Defendants’ Motion to Dismiss the Amended Complaint, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, March 22, 2024.

password best practices, for instance, by storing hard-coded passwords in configuration files in plaintext. Similarly, contrary to the Security Statement, senior SolarWinds employees were aware that complex passwords were not uniformly enforced.

- c. The practices SolarWinds described in internal documents were inconsistent, from a cybersecurity perspective, with certain assertions made in the Security Statement regarding the **development of secure software**. SolarWinds did not, in the manner that was represented in the Security Statement, follow a defined methodology for developing secure software, follow standard security practices, or maintain separate development and production environments.

27. SolarWinds was internally aware that the company departed from well-accepted cybersecurity norms. By failing to apply the controls described in the Security Statement in a consistent manner, SolarWinds amplified the company's cybersecurity risks.

28. Many of the cybersecurity norms that SolarWinds violated were elementary in nature, part of the fundamental blocking and tackling that constitutes everyday cybersecurity. For example, the need to separate production and development environments is so fundamental that I teach this to my students as part of my introductory undergraduate System Security class. The fact that such simple issues slipped through the company's internal systems should have alerted SolarWinds' cybersecurity leadership of potential systemic issues. Based on my over 40 years of experience, the existence of such basic issues also should have alerted SolarWinds' cybersecurity leadership that the Security Statement—which categorically described conformity with industry best practices—was inaccurately describing SolarWinds' cybersecurity posture.

III. FACTUAL BACKGROUND

A. General Background on Cybersecurity and the Cybersecurity Practices of Corporations

29. Cybersecurity is the process of protecting information, data, networks, and devices from unauthorized access, and ensuring the confidentiality, integrity, and availability of information.²⁷ In this section, I describe cybersecurity concepts and best practices to which I refer throughout my expert report, as established by the cybersecurity industry and based on my own experience.

30. The cybersecurity of an organization can often be compromised via the intentional exploitation of a vulnerability (a security weakness).²⁸ When bad actors exploit a vulnerability as one element of a cyberattack, this can lead to a security breach, in which an unauthorized person can access, steal, view, modify, or destroy data (or disrupt operations).²⁹

31. As security breaches can have substantial financial and reputational consequences, cybersecurity processes and practices aim to prevent, detect, and respond to cyberattacks.³⁰ Organizations may designate a senior executive, known as the Chief Information

²⁷ CISA, “What is Cybersecurity?,” February 01, 2021, <https://www.cisa.gov/news-events/news/what-cybersecurity>.

²⁸ NIST, *NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations*, September 2020 (“NIST Special Publication 800-53”), p. 423. (A vulnerability is a “[w]eakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.”).

²⁹ NIST Special Publication 800-53, pp. 151, 154. (“A breach results in the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or a similar occurrence where a person other than an authorized user accesses or potentially accesses personally identifiable information” and “could potentially affect the organization’s operations, assets, and individuals.”).

³⁰ Cybersecurity is defined as “[t]he process of protecting information by preventing, detecting, and responding to attacks.” NIST Cybersecurity Framework, p. 45.

Security Officer (CISO), to oversee the development and implementation of cybersecurity policies.³¹

32. Although all complex systems will likely carry vulnerabilities (and can therefore never achieve perfect cybersecurity), the cybersecurity community has developed widely-accepted industry norms and best practices for managing—and, often, reducing—the risks of a cyberattack.

33. First, there are several organizations that provide guidance on how to develop, acquire, operate, and maintain secure software products and cybersecurity practices. For example, in the United States, the National Institute of Standards and Technology (NIST) “develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies and the broader public.”³² In addition, operating as a component of the United States Department of Homeland Security, the Cybersecurity & Infrastructure Security Agency (CISA) is the “operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience.”³³ Globally, the Open Worldwide Application Security Project (OWASP) provides organizations with security recommendations.³⁴ More generally, the International Organization for Standardization’s (ISO) ISO 27001 standard provides internationally recognized standards for IT security, cybersecurity

³¹ CISCO, “What Is a CISO?,” <https://www.cisco.com/c/en/us/products/security/what-is-ciso.html>.

³² NIST, “Cybersecurity,” <https://www.nist.gov/cybersecurity>.

³³ CISA, “About CISA,” <https://www.cisa.gov/about>; The Department of Homeland Security, “Operational and Support Components,” <https://www.dhs.gov/operational-and-support-components>.

³⁴ The Open Worldwide Application Security Project is “a nonprofit foundation that works to improve the security of software.” OWASP, “About the OWASP Foundation,” <https://owasp.org/about>.

and privacy protection.^{35,36} The SANS Institute and the Center for Internet Security (CIS) also provide useful and reliable information about best practices in cybersecurity.^{37,38}

34. Second, organizations also provide guidance on known vulnerabilities and how to respond to them. The CERT Coordination Center (CERT/CC) focuses on researching software vulnerabilities, publishing findings, and coordinating responses to security incidents.³⁹ The Forum of Incident Response and Security Teams (FIRST), which I had the honor to chair some years ago, maintains the Common Vulnerability Scoring System (CVSS), which provides a standardized way to capture the characteristics of vulnerabilities and thus allows accurate prioritization of addressing them.⁴⁰

35. Third, commonly accepted principles help guide organizations in managing cyberattacks. For example:

- a. The principle of “defense-in-depth” states that organizations should apply multiple security layers to ensure that vulnerabilities not remediated by one

³⁵ The official name of this standard is ISO/IEC 27001, and it forms part of the ISO/IEC 27000 family of standards. According to the ISO, “ISO/IEC 27001 is the world’s best-known standard for information security management systems (ISMS) and their requirements.” See ISO, “Information Security,” <https://www.iso.org/sectors/it-technologies/information-security>; ISO, “ISO/IEC 27000 Family,” <https://www.iso.org/standard/iso-iec-27000-family>.

³⁶ As the ISO 27001 was updated in 2022, throughout my expert report I refer to the 2013 version, which was applicable during the Relevant Period. ISO, *ISO/IEC 27001:2022: Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements*, October 2022; ISO, *ISO/IEC 27001:2013(E): Information Technology — Security Techniques — Information Security Management Systems — Requirements*, October 01, 2013 (“ISO/IEC 27001:2013(E)”).

³⁷ SANS Institute, “About SANS Institute,” <https://www.sans.org/about>.

³⁸ CIS, “The 20 CIS Controls & Resources,” *available on* June 19, 2019, <https://web.archive.org/web/20190619213638/https://www.cisecurity.org/controls/cis-controls-list/>.

³⁹ Software Engineering Institute, “CERT Coordination Center”, <https://www.sei.cmu.edu/about/divisions/cert/index.cfm>.

⁴⁰ First, “Common Vulnerability Scoring System SIG,” <https://www.first.org/cvss/>.

countermeasure are addressed by another.⁴¹ For example, in addition to deploying firewalls, organizations typically also protect their sensitive data through access controls⁴² to ensure that, even if bad actors succeed in bypassing the firewall, they are prevented from accessing the data.

- b. The principle of “least privilege” states that each person, program, or entity should be granted the minimum amount of privilege (*i.e.*, access to system resources and authorizations) that the person, program, or entity needs to perform its necessary functions.⁴³ In practice, this principle is often implemented through access controls. For example, organizations may issue unique credentials (usernames and passwords) to each employee to ensure that only those employees access certain databases whose role necessitates using the database.⁴⁴
- c. The principle of “separation of duties” states that no one person should be given enough privileges to have the power to (accidentally or purposefully) misuse the system, *i.e.*, no one person should have too much authority.⁴⁵

⁴¹ NIST, “Glossary – ‘Defense-in-Depth’,” https://csrc.nist.gov/glossary/term/defense_in_depth.

⁴² NIST defines access controls as “[a]ccess privileges granted to a user, program, or process or the act of granting those privileges.” NIST, “Glossary – ‘Access Control’,” https://csrc.nist.gov/glossary/term/access_control.

⁴³ NIST, “Glossary – ‘Least Privilege’,” https://csrc.nist.gov/glossary/term/least_privilege.

⁴⁴ Saltzer, Jerome H. and Michael D. Schroeder, “The Protection of Information in Computer Systems,” *Proceedings of the IEEE*, Vol. 63, No. 9, September 1975, pp. 1278–1308, p. 1282. (“Every program and every user of the system should operate using the least set of privileges necessary to complete the job. Primarily, this principle limits the damage that can result from an accident or error. It also reduces the number of potential interactions among privileged programs to the minimum for correct operation, so that unintentional, unwanted, or improper uses of privilege are less likely to occur.”).

⁴⁵ NIST, “Glossary – ‘Separation of Duty (SOD)’,” https://csrc.nist.gov/glossary/term/separation_of_duty. *See also*, ISO/IEC 27001:2013(E), A.6.1.2.

B. Background on SolarWinds

36. In this section, I provide a brief background on SolarWinds as described on the SolarWinds website during the Relevant Period.⁴⁶

37. During the Relevant Period, SolarWinds' products served approximately 275,000 customers globally,⁴⁷ including, small businesses, large enterprises, and government organizations.⁴⁸

38. SolarWinds offered a range of IT management products designed to help businesses with their "network management," "systems management," "IT security," "database management," "IT help desk," and "DevOps" [software development and IT operations] needs.⁴⁹ SolarWinds enabled its customers to monitor and manage their IT environments on-premises, in the cloud, and in hybrid environments.⁵⁰ Additionally, SolarWinds also offered its customers a technology platform known as the SolarWinds Orion Platform, which enabled customers to view

⁴⁶ Following the 2020 "Sunburst" attack, SolarWinds rebranded and transformed some of its products and services. *See, e.g.*, SolarWinds, "SolarWinds Transforms Brand to Signify Ongoing Evolution, Portfolio Expansion, and Customer Empowerment," May 30, 2023, <https://investors.solarwinds.com/news/news-details/2023/SolarWinds-Transforms-Brand-to-Signify-Ongoing-Evolution-Portfolio-Expansion-and-Customer-Empowerment/default.aspx>. *See also*, Johnson, Tony, "New and Improved SolarWinds Platform, Who Dis?," THWACK, April 20, 2022, <https://thwack.solarwinds.com/products/the-solarwinds-platform/b/news/posts/new-and-improved-solarwinds-platform-who-dis>.

⁴⁷ SolarWinds, "Corporate Overview," *available on* April 30, 2019, <http://web.archive.org/web/20190430082154/https://investors.solarwinds.com/overview/default.aspx>.

⁴⁸ SolarWinds, "SolarWinds Sets Its Sights on the ITSM Market through Acquisition of Samanage and Introduction of a SolarWinds Service Desk Product," April 11, 2019, <https://investors.solarwinds.com/news/news-details/2019/SolarWinds-Sets-Its-Sights-on-the-ITSM-Market-through-Acquisition-of-Samanage-and-Introduction-of-a-SolarWinds-Service-Desk-Product/default.aspx>; Cimpanu, Catalin, "SEC Filings: Solarwinds Says 18,000 Customers Were Impacted by Recent Hack," ZDNET, December 14, 2020, <https://www.zdnet.com/article/sec-filings-solarwinds-says-18000-customers-are-impacted-by-recent-hack/>.

⁴⁹ SolarWinds, "IT Management Software & Monitoring Tools," *available on* April 30, 2019, <http://web.archive.org/web/20190430194414/https://www.solarwinds.com>.

⁵⁰ SolarWinds, "Corporate Overview," *available on* April 30, 2019, <http://web.archive.org/web/20190430082154/https://investors.solarwinds.com/overview/default.aspx>.

and experience many different SolarWinds products in a single platform.^{51,52} SolarWinds' products were principally built by the SolarWinds engineering teams.⁵³

39. Additionally, SolarWinds also developed software for internal use. These internal solutions, to which SolarWinds referred as Business Applications ("BizApps"), were not directly sold to customers; instead, they supported SolarWinds' internal functions such as billing and collecting information from customers.⁵⁴ For example, a BizApp known as the Orion Improvement Platform ("OIP") collected information from customers "evaluation, performance, and data from SolarWinds users to determine ways [SolarWinds] products may be improved."⁵⁵ OIP therefore gave SolarWinds access to sensitive customer data including user identification, user device, and Orion and SolarWinds product-specific usage data.⁵⁶ Such information is

⁵¹ SolarWinds, "Orion Platform - Scalable IT Monitoring," *available on* April 30, 2019, <http://web.archive.org/web/20190430082356/https://www.solarwinds.com/solutions/orion>.

⁵² After the Relevant Period, the Orion Platform was transformed and rebranded as the SolarWinds Platform. *See* Johnson, Tony, "New and Improved SolarWinds Platform, Who Dis?," THWACK, April 20, 2022, <https://thwack.solarwinds.com/products/the-solarwinds-platform/b/news/posts/new-and-improved-solarwinds-platform-who-dis>.

⁵³ Investigative Testimony of Kevin Thompson - Vol. I, September 1, 2022 ("Investigative Testimony of Kevin Thompson - Vol. I") at 82:8-15. ("If it's product development, it would be the environment that our engineers were using to [...] write the code for the products that the company was selling[.]").

⁵⁴ Investigative Testimony of Timothy Brown - Vol. II, March 9, 2022 ("Brown Investigative Testimony, Vol. II") at 394:20-395:12. ("We have a number of internally built solutions, [...] that do things like support our billing, that help us manage our customers, that help us generate lists of customers to send emails to. So these are called Bizapps, business applications."). It appears that the term "BizApps" referred both to the business applications and to the team that created these applications. *See* Brown Deposition at 270:23-271:9. ("Q. [...] What is BizApps in your understanding? A. So BizApps is a group that reported to Rani Johnson. BizApps were produced internal products or internal solutions. [...] Q. So were the BizApps sold to customers or were they just solely used within SolarWinds? A. Solely used within SolarWinds.").

⁵⁵ SolarWinds, "Orion Improvement Program," first published on October 15, 2018, last published on January 7, 2022, https://solarwindscore.my.site.com/SuccessCenter/s/article/Orion-Improvement-Program?language=en_US. *See also*, Brown Investigative Testimony, Vol. II at 395:4-7. ("OIP [...] was built internally for the specific purpose of collecting information and helping customers with their deployment.").

⁵⁶ SolarWinds, "Orion Improvement Program," first published on October 15, 2018, last published on January 7, 2022, https://solarwindscore.my.site.com/SuccessCenter/s/article/Orion-Improvement-Program?language=en_US. ("[T]he following is an example of data collected [...] when you participate in the Orion Improvement Program: •The SWID (SolarWinds ID) associated with any SolarWinds commercial licenses installed. •The email address provided to the installer during installation. [...] •Operating system version. •CPU description and count. •Physical

sensitive data because it could be attractive for an attacker to steal information about customer identities and the devices on the customer network. This data is also business-sensitive information because the identities of customers and their systems may not be information that customers want to be made public.

40. In **Table 1** below, I have summarized some of the cybersecurity and leadership personnel at SolarWinds during the Relevant Period.

Table 1

Name	Position(s) During Relevant Period
Timothy Brown	Head of the Information Security Group (“InfoSec”) and Vice President of Security and Architecture
Jason Bliss	Chief Administrative Officer (“CAO”) and General Counsel
Brad Cline	Director and Senior Director of IT
Steven Colquitt	Senior Director of Software Engineering
Chris Day	VP of Global DevOps and Technology Operations
Harry Griffiths	Technical Support Engineer of Customer Support Group and Incident Response Engineer
Rani Johnson	Chief Information Officer (“CIO”) and Head of DevOps and IT Group (“DOIT”)
Joseph Kim	Chief Technology Officer (“CTO”) and Executive Vice President of Engineering
Kellie Pierce	Director of Security, Privacy and Compliance, InfoSec
Eric Quitugua	Senior Manager of Security Operations, InfoSec
Kevin Thompson	Chief Executive Officer (“CEO”)

memory installed and percent used. [...] •Dates when you logged in to the Orion website. •Licensing information of other SolarWinds Orion products locally installed. [...] •Data about devices and applications monitored: ◦Vendor[,] ◦Model[,] ◦OS/Firmware version[,] ◦Count[,] ◦Abstract configuration information, such as number of websites hosted[,] •Data about the SolarWinds product: ◦Feature usage statistics[,] ◦Performance statistics[,] ◦Hardware and OS platform description”).

IV. ANALYSIS AND OPINIONS

A. Research Methodology and Analytical Framework

41. As I described above, I have been retained to provide my analysis and opinions on a technical comparison between the state of cybersecurity depicted in (1) the publicly available SolarWinds Security Statement and (2) SolarWinds’ internal assessments, presentations, and communications with respect to the following four main areas of focus: access control, user authentication, secure development lifecycle, and network monitoring.

42. Throughout my expert report, I refer to SolarWinds’ public “Security Statement” published on its website. Based on the documents reviewed to date, my understanding is that SolarWinds’ “Security Statement” was first published on its website on November 16, 2017,⁵⁷ and that it remained substantially unchanged throughout the Relevant Period.^{58,59}

⁵⁷ SW-SEC00337101–109 (Email from Tim Brown attaching SolarWinds Security Statement, Oct 13–Nov 7, 2017) at 101 (On November 7, 2017, Tim Brown circulated a Security Statement noting it “has been approved by legal and is in the process of being made available via the website.”); SW-SEC00466120–142 (SolarWinds’ Security Statement) (Emails discussing the publication of the Security Statement on the website, Nov 7–Dec 27, 2017) at 123 (On November 16, 2017, a SWI employee confirmed: “This went live today”).

⁵⁸ SolarWinds Corp.’s Responses and Objections to Plaintiff’s First Requests for Admission to Defendant SolarWinds Corp, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, May 17, 2024 (“Responses and Objections”), p. 3. (“REQUEST FOR ADMISSION NO. 2: Admit that SolarWinds’ Security Statement was continuously available on its publicly available website in substantially identical form from December 31, 2017 through December 14, 2020. RESPONSE TO REQUEST FOR ADMISSION NO. 2: Admit.”). *See, e.g.*, SW-SEC00337101–109.

⁵⁹ I also understand that (at least as of May 2018), SolarWinds provided to its customers a more detailed Security Statement upon request for additional information regarding security practices. I have not yet seen documents indicating whether this detailed security statement was publicly available. For this reason, I have focused my analysis only on those statements that have been made in the publicly-available Security Statement. SW-SEC00292763–781 (Detailed SolarWinds Security Statement dated May 2018, shared by Tim Brown via email on April 16, 2019); SW-SEC00010210–229 (Email exchange attaching Detailed SolarWinds Security Statement, dated May 2018) at 210. (Email from Eric Quitugua on September 11, 2018, “For any future inquiries or requests to complete similar assessments/questionnaires, please refer the customer to the SolarWinds security statement at [SolarWinds website URL] [...]. If a current customer make [sic] a request to provide more detailed responses after sharing the URL, we can go ahead and share our detailed security statement that is marked as confidential.”). *See also*, Investigative Testimony of Eric Quitugua - Vol. I, August 31, 2021 (“Quitugua Investigative Testimony, Vol. I”) at 123:19–124:10.

43. The Security Statement—explicitly and implicitly—refers to specific cybersecurity terminology, standard practices, and industry norms. For example, it states that “SolarWinds follows the NIST Cybersecurity Framework,” “SolarWinds’ secure development lifecycle follows standard security practices,” and “security best practices are a mandated aspect of all development activities.”⁶⁰ Therefore, rather than in a vacuum, I interpreted the Security Statement in the context of the cybersecurity-related guidance, best practices, and standards provided by well-accepted industry leading organizations such as those that I described in **Section III.A** (including NIST, the ISO, and CERT/CC).

44. Throughout my expert report, with respect to the four areas of focus in my assignment, I evaluated SolarWinds’ cybersecurity posture described in the Security Statement based on my interpretation of the guidelines described by organizations such as NIST, as well as my first-hand experience with the implementation of well-accepted industry norms. Similarly, I applied the same industry norms when interpreting SolarWinds’ cybersecurity practices, as depicted in the internal documents. Using this framework, I compared the state of cybersecurity described in the Security Statement with the state of cybersecurity depicted in SolarWinds’ internal documents.

45. Specifically, to make this comparison with respect to each of the four areas, my analysis consisted of the following steps:

⁶⁰ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 129, 132.

- a. First, I reviewed the Security Statement, identifying those assertions within the ambit of the four areas which were sufficiently definite—that is, categorical—as to be either intrinsically verifiable or falsifiable.⁶¹
- b. Second, I evaluated whether the practices described in the verifiable/falsifiable assertions were consistent with widely accepted industry norms. I relied on my many years of experience, as well as my familiarity with documented industry norms, described later herein, to make these judgments.
- c. Third, to evaluate whether the internal SolarWinds documents depict a state of cybersecurity consistent with the Security Statement, I needed to know which evidentiary documents discuss the relevant topics. I therefore created a set of key words and terms that, based on my experience, I considered to relate to each of the four areas I have been assigned to investigate. I asked my team to search the production documents for these terms. I also asked counsel to provide me with types of production documents that, based on my experience, I considered to be relevant to evaluate SolarWinds’ internal understanding of its cybersecurity posture. For example, following my request, counsel provided me with Risk Acceptance Forms.⁶² I also reviewed investigative and deposition testimony from

⁶¹ For example, I find the following sentence too vague to be verifiable: “SolarWinds employees are required to conduct themselves in a manner consistent with the company’s guidelines, including those regarding confidentiality, business ethics, appropriate usage, and professional standards.” SW-SEC00466120–142 (SolarWinds’ Security Statement) at 130. As I described above, in my statement that certain phrases or sentences are “not verifiable,” I mean this from a cybersecurity perspective. I’m not offering a legal opinion as to whether they could be a materially misleading statement.

⁶² Like many other organizations, SolarWinds used Risk Acceptance Forms (“RAF”) to document risks and vulnerabilities expected to persist for a longer period of time. Through this process, SolarWinds defined a timeline for risks to be remediated. The RAF process is common: when organizations identify risks through the course of their software development process, they may decide to mitigate or to accept the identified risks based on the severity of the risk and on the organizations’ risk tolerance. *See* SW-SEC00168009–017 at 011. (“This Risk

SolarWinds employees to better understand the context of these internal documents.

- d. Fourth, I reviewed these internal documents and testimony transcripts to evaluate, based on my experience, whether they depicted a state of cybersecurity consistent with the assertions in the Security Statement.

46. Let me note that it was not necessary to review all SolarWinds internal documents related to a topic for me to reach a conclusion about whether the internal documents depicted a state of cybersecurity consistent with the assertions in the Security Statement. I have found evidence of many flaws in SolarWinds' practices, and they are sufficient in the aggregate for me to conclude that SolarWinds did not consistently implement the practices described in several assertions in the Security Statement. Reviewing additional documents would not have changed my opinion because the flaws that I have found were so consequential in the aggregate that, from a cybersecurity perspective, they placed the company (and, in some cases, its customers) at profound cybersecurity risk and directly contradicted several assertions in the Security Statement. Even if I had found a large number of additional internal documents describing SolarWinds adhering to industry norms at times, these would not have changed my opinions. By way of analogy, if the front door is unlocked, being sure that all windows are closed will not ensure that the house is protected from burglars.

47. It is also important to observe that many of the assertions in the Security Statement were categorical and unqualified. The Security Statement contained little qualifying

Acceptance Form (RAF) is to be used in instances where the risk is likely to exist for more than 1 month and/or if risk actualized, the event would trigger our security incident response process. The RAF must be approved by the SolarWinds Executive (Vice President or higher) responsible for the asset or service accepting the risk.”). *See also*, NIST, *NIST Special Publication 800-37: Risk Management Framework for Information Systems and Organizations*, NIST, December 2018 (“NIST Special Publication 800-37”), p. 72.

language indicating that assertions of the Security Statement might not be consistently followed. For example, while the Security Statement noted that “SolarWinds **strives** to apply the latest security patches and updates,”⁶³ it did not use similar language (such as “strives”) with respect to the other assertions. In fact, many sentences explicitly used language indicating categorical assertions, such as “By default, **all** access is denied,” “Our password policy covers **all** applicable information systems,” and “Quality Assurance is involved at **each** phase of the lifecycle and security best practices are a **mandated** aspect of **all** development activities” [Emphasis added].⁶⁴ Based on my experience with security statements and how organizations discuss cybersecurity practices, when organizations make such categorical and unqualified assertions about their cybersecurity practices, I interpret this to mean that such practices are consistently followed.

48. Considering the evidence I have seen and based on my experience in evaluating the cybersecurity practices of large organizations, I am of the opinion that the state of cybersecurity depicted in SolarWinds’ internal discussions did not match several of the very broad, categorical and unqualified assertions in the Security Statement. My main conclusion, therefore, is that several of the cybersecurity issues raised in these internal documents indicate that SolarWinds failed to consistently apply the cybersecurity practices described in the Security Statement.

⁶³ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132. Emphasis added.

⁶⁴ See: “Our security policies cover a wide array of security related topics ranging from general standards with which **every** employee must comply”. “Network components, workstations, applications and **any** monitoring tools are enabled to monitor user activity.” “**All** newly hired employees are required to sign confidentiality agreements and to acknowledge the SolarWinds code of conduct policy.” “SolarWinds maintains a change management process to ensure that **all** changes made to the production environment are applied in a deliberate manner.” “By default, **all** access is denied and only explicitly allowed ports and protocols are allowed based on business need.” “Our password policy covers **all** applicable information systems, applications, and databases.” “Quality Assurance is involved at **each** phase of the lifecycle and security best practices are a mandated aspect of **all** development activities.” “**Each** vulnerability is reviewed to determine if it is applicable, ranked based on risk, and assigned to the appropriate team for remediation.” SW-SEC00466120–142 (SolarWinds’ Security Statement) at 129-132. Emphasis added.

49. Simply put, there were significant cybersecurity practices that SolarWinds claimed to follow that the company did not consistently follow. Additionally, internal SolarWinds documents suggest that the deficiencies and omissions were presented to the relevant cybersecurity personnel and, in many cases, company leadership.

50. My decades of experience have taught me that no organization has perfect cybersecurity and that any organization diligently assessing its cybersecurity will uncover, from time to time, some issues needing to be addressed. However, the cybersecurity problems that I explain in this expert report, reflected in the SolarWinds internal documents and testimony, do not constitute the kind of routine minor problems that a company would encounter if it followed security best practices and industry norms in the manner described in the Security Statement. In my opinion, the discrepancies between SolarWinds' internal documents and Security Statement within the areas of access control, user authentication, and secure development lifecycle processes are reflective of significant deviations from industry norms, with potential company-wide impact, and in some cases an impact on the security of its customers as well.

51. I describe my detailed findings in the remainder of my report.

B. SolarWinds Internal Documentation and Testimony Show That SolarWinds Did Not Consistently Follow the Assertions in the Security Statement Regarding Access Controls

52. As I show below, my opinion is that the practices SolarWinds described in internal documents were inconsistent, from a cybersecurity perspective, with certain access control related assertions made in the Security Statement. Notably, based on the internal SolarWinds documents that I have reviewed, my conclusion is that SolarWinds was internally

aware of significant access control problems that substantially raised the company's cybersecurity risk profile.

53. In this section, I first provide an overview of access controls within the context of cybersecurity (**Section IV.B.1**). Second, I present potentially verifiable (or falsifiable) assertions made by SolarWinds in its public Security Statement concerning access controls (**Section IV.B.2**). Third, I interpret both the Security Statement and SolarWinds' internal documents describing access controls in the context of the well-accepted industry norms that were available during the Relevant Period. As I described in **Section IV.A**, these industry norms represent the context of the Security Statement. Based on my first-hand experience with these industry norms, as well as my interpretation of the guidance from industry bodies described below, I find that internal communications within SolarWinds revealed employee awareness of the company's inconsistent implementation of these access controls and that SolarWinds failed to meet widely accepted industry norms (**Section IV.B.3**).

1. Introduction to access control

54. Access controls determine who has access to what data, systems, and related applications, and under what circumstances. In other words, the goal of access control is to ensure that only authorized persons can access the organization's data, systems, and related applications.⁶⁵ Access controls therefore play a critical role in protecting organizations against

⁶⁵ NIST Special Publication 800-53, p. 23. ("Access control policies control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (i.e., devices, files, records, domains) in organizational systems. In addition to enforcing authorized access at the system level[,] [...] access enforcement mechanisms can also be employed at the application and service level to provide increased information security and privacy.").

breaches and other forms of cyberattacks. For this reason, issues with access control can cause serious vulnerabilities, as NIST, for example, warns.⁶⁶

55. The “principle of least privilege” and the concept of “role-based access”—which, as I explain below, the Security Statement states that SolarWinds followed—are foundational in securing sensitive data and preventing unauthorized access to a company’s network.⁶⁷ To conform to the principle of least privilege, some organizations enact a “need-to-know” access control policy, where individuals have access to the minimum amount of information necessary to execute their work.⁶⁸ Similarly, in a role-based access control model, users’ access to information is determined by their role within the organization.⁶⁹ For instance, a network administrator may have full (“read,” “write,” and “edit”) permissions to company data, whereas a standard user account may be restricted to read-only access by default.⁷⁰

56. As I explained in the *CISSP Official Reference* Chapter on “Identity and Access Management,” to implement access controls, organizations typically rely on a combination of access control mechanisms, such as:

⁶⁶ NIST, “Access Control Policy Testing,” available on October 18, 2019, <https://web.archive.org/web/20191018185137/https://csrc.nist.gov/projects/access-control-policy-tool>. (“Often a system’s privacy and security are compromised due to the misconfiguration of access control policies instead of the failure of cryptographic primitives or protocols.”).

⁶⁷ I explain the “principle of least privilege” in more detail **Section III.A**. See also, Saltzer, Jerome H. and Michael D. Schroeder, “The Protection of Information in Computer Systems,” *Proceedings of the IEEE*, Vol. 63, No. 9, September 1975, pp. 1278–1308.

⁶⁸ NIST Special Publication 800-53, pp. 36, 38. (“Organizations employ least privilege for specific duties and systems. The principle of least privilege is also applied to system processes, ensuring that the processes have access to systems and operate at privilege levels no higher than necessary to accomplish organizational missions or business functions. [...] Policies and procedures for granting equivalent status of employees to individuals include a need-to-know, citizenship, and the relationship to the organization.”).

⁶⁹ See, e.g., Warsinske et al. (2019) Chapter 5 - Identity and Access Management, p. 528. (“R[ole-]B[ased] A[ccess] C[ontrol] is an access control model that bases the access control authorizations on the roles (or functions) that the user is assigned within an organization.”). See also, NIST, “Role Based Access Control,” June 22, 2020, <https://csrc.nist.gov/projects/role-based-access-control>; and NIST Special Publication 800-53, p. 415.

⁷⁰ See, e.g., Warsinske et al. (2019) Chapter 5 - Identity and Access Management, pp. 528-529.

- a. Physical access control mechanisms, including keycards and security personnel protecting data server rooms;⁷¹
- b. Administrative access control mechanisms, including conducting background checks on new hires;⁷² and
- c. Technical access control mechanisms, including authenticating the identity of a user through mandatory credentials such as passwords and limiting network access through firewalls.⁷³

2. *The SolarWinds Security Statement made assertions about access control*

57. Among other things, the Security Statement stated the following with respect to access control:

- a. “Access controls to sensitive data in our databases, systems, and environments are **set on a need-to-know / least privilege necessary basis.**”⁷⁴
- b. “**Role based access controls** are implemented for access to information systems. [...] SolarWinds employees are granted a limited set of default permissions to access company resources, such as their email, and the corporate intranet. Employees are granted access to certain additional resources **based on their**

⁷¹ See, e.g., Warsinske et al. (2019) Chapter 5 - Identity and Access Management, pp. 484, 488-489. See also, U.S. Department of Homeland Security, *Access Control Technologies Handbook*, September 2015, pp. 1, 18-19.

⁷² See, e.g., Warsinske et al. (2019) Chapter 5 - Identity and Access Management, pp. 513-514.

⁷³ See, e.g., Warsinske et al. (2019) Chapter 5 - Identity and Access Management, pp. 493, 522, 529.

⁷⁴ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132. Emphasis added.

specific job function. Requests for additional access **follow a formal process** [...].”⁷⁵

- c. “Processes and procedures are in place to address **employees who are voluntarily or involuntarily terminated.**”⁷⁶

58. Additionally, the Security Statement also specified that “SolarWinds’ data and information system assets are comprised of **customer and end-user assets as well as corporate assets.** These asset types are managed under our security policies and procedures.”⁷⁷ It is therefore my understanding that the assertions regarding access controls applied to “customer and end-user assets as well as corporate assets,” and my comments in this section pertain to both.

3. *SolarWinds failed to follow access control practices asserted in the Security Statement*

59. Despite the above public assertions, internal SolarWinds communications and testimony indicate that the actual practices at SolarWinds over the Relevant Period were inconsistent with the statements described in the Security Statement.

60. Below, I first describe examples where SolarWinds’ internal documents indicate that the company’s practices did not consistently conform to the Security Statement’s assertions regarding access control (**Sections IV.B.3.a-c**). Then, in **Section IV.B.3.d**, I discuss in detail the implications and potential consequences of access control violations. As I will show, industry bodies such as NIST, ISO, SANS, CERT/CC, and CISA agree that a failure to follow commonly accepted access control practices, such as the principle of least privilege, can expose the

⁷⁵ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132. Emphasis added.

⁷⁶ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132. Emphasis added.

⁷⁷ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 129. Emphasis added.

organization to several types of risks, including, among others: (1) increased exposure to external attacks; (2) increased risk of insider threats; (3) increased difficulty with preventing, detecting, and responding to cyberattacks; and (4) other operational risks.⁷⁸ In addition, it can lead to regulatory non-compliance.⁷⁹

a. Internal documents contradicted the assertion that SolarWinds' access controls are set on a "need-to-know / least privilege necessary" basis

61. In direct contradiction with the public statement that access controls are “set on a need-to-know / least privilege necessary basis,” an internal document circulated by Mr. Brown on March 15, 2018 indicated that the “[c]oncept of least privilege [was] not followed as a best practice.”⁸⁰ This statement—*i.e.*, that least privilege was not followed as a best practice—is corroborated by Mr. Quitugua’s testimony that, at least as of early 2018, SolarWinds identified

⁷⁸ NIST Special Publication 800-53, p. 38 (“The misuse of privileged functions, either intentionally or unintentionally by authorized users or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Logging and analyzing the use of privileged functions is one way to [...] help mitigate the risk from insider threats and the advanced persistent threat.”); ISO/IEC 27001:2013(E), A.9.2 (“The allocation and use of privileged access rights shall be restricted and controlled” with the objective “to prevent unauthorized access to systems and services.”); Shackleford, Dave and Arick Goomanovsky, “Mitigate Access Risk by Enforcing Least Privilege in Cloud Infrastructure,” SANS, September 16, 2020, <https://www.sans.org/webcasts/mitigate-access-risk-enforcing-privilege-cloud-infrastructure-116290/> (“[D]evelopers tend to grant broad entitlements, resulting in ‘permission creep’ which is very difficult to eliminate in production. As many as 90% of these permissions are unused, excessive, and a tremendous risk to the environment.”); Miller, Sarah, “Separation of Duties and Least Privilege (Part 15 of 20: CERT Best Practices to Mitigate Insider Threats Series),” SEI, July 26, 2017 <https://insights.sei.cmu.edu/blog/separation-of-duties-and-least-privilege-part-15-of-20-cert-best-practices-to-mitigate-insider-threats-series/> (“In addition to protecting against malicious attacks, separation of duties and least privilege also assists in mitigating unintentional insider threats.”); CISA, “Technical Approaches to Uncovering and Remediating Malicious Activity,” September 24, 2020, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-245a> (“Decrease a threat actor’s ability to access key network resources by implementing the principle of least privilege.”).

⁷⁹ See, e.g., *Sarbanes-Oxley Act of 2002* (“Sarbanes-Oxley Act”) § 404. Management Assessment of Internal Controls. See also, *Article 32 of the General Data Protection Regulation (GDPR): Security of Processing* (“GDPR Article 32”); ISO/IEC 27001:2013(E), A.18.1.3. (“Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislative, regulatory, contractual and business requirements.”).

⁸⁰ SW-SEC00012265–275 (Email with subject “Security Projects - Mar 2018 Tim’s changes.pptx,” with presentation attached, March 15, 2018) at 268.

“as part of [its] internal audits and checks that not all systems [...] were following [the concept of least privilege] best practice.”⁸¹

62. Similarly, an internal presentation from August 2019 reported the following: “Access and privilege to critical systems / data is inappropriate. Need to improve internal processes | procedures.”⁸² Indeed, when asked about this statement in his deposition, Mr. Brown admitted that the process that granted people access to systems “wasn’t a hundred percent perfect,” and that some people may have had access to systems to which they should not have.⁸³ If people have access to “critical systems / data” that should fall outside of their scope of privilege then, by definition, the organization is not successful in setting access controls “on a need-to-know” basis, as the Security Statement asserted.⁸⁴ Simply put, if—as Mr. Brown testified—it was possible that “somebody had access that shouldn’t have been there,”⁸⁵ then that person was allowed to have access to information that he or she did not *need to know*.

63. This failure is important. While of course many processes are not “a hundred percent perfect,” the decisive consideration is the level of importance of the things that are allowed to fall through the cracks. As I described above, based on SolarWinds’ own internal

⁸¹ Investigative Testimony of Eric Quitugua - Vol. II, September 1, 2021 (“Quitugua Investigative Testimony, Vol. II”), at 280:13-281:4. (“Q. In this early 2018 timeframe, was the concept of least privilege not being followed throughout the SolarWinds organization? A. We identified, you know, as part of our internal audits and checks that not all systems which were under IT control were following best practice. Q. Okay. And I think we had looked again previously at the detailed security statement, and the detailed security statement indicated that SolarWinds did follow the concept of least privileged, correct? A. Yes. Q. So what you’re telling me is that at least with respect to some systems, that wasn’t the case? A. For a subset of systems that we identified, they weren’t -- you know, for whatever reason, we identified that they weren’t following the best practices that we described.”).

⁸² SW-SEC00001497–550 (Presentation, “Security & Compliance Program Quarterly Overview,” August 16, 2019) at 507.

⁸³ Brown Deposition at 203:12-18. (“[Mr. Brown:] What I can say is that we had processes in place to grant people access to systems in an appropriate way. [...] It wasn’t a hundred percent perfect. An audit may show something that somebody had access that shouldn’t have been there.”).

⁸⁴ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132.

⁸⁵ Brown Deposition at 203:12-18.

document, as of August 2019, it was the access management to “critical” systems and data that was inappropriate [emphasis added]. In my experience, in cybersecurity, the word “critical” is carefully applied to mean issues that affect whether or not the mission can be completed. If a problem is described as “critical,” this implies that a catastrophic loss may occur.⁸⁶ As a result, whenever critical problems are involved, perfection, or at a minimum urgent remediation, is highly important. The Security Statement’s categorical assertion that “access controls are [...] set on a need-to-know / least privilege necessary basis” is, in my opinion and experience, contradicted by the evidence shown in the August 2019 presentation and Mr. Brown’s acknowledgement of these flaws.

64. Around the same time, an internal assessment of security controls prepared by Ms. Pierce and shared with Mr. Brown and Ms. Johnson in August 2019 found similar problems.⁸⁷ Ms. Pierce defined three possible states for these controls she reviewed. She characterized them as either “Program/Practice in place,” “Program/Practice may be in place but requires detailed review,” or “No program/practice in place.”⁸⁸ I note that, of the three possible states, only the first affirmatively denotes that the program or practice is in place. Of the 43 controls considered in the “Access Control” Family,⁸⁹ only two were rated this way. A further 18 were rated “Program/Practice may be in place but requires detailed review.” Another 23 access

⁸⁶ I note that imperfect execution of these controls might also lead to non-critical events.

⁸⁷ SW-SEC00045358 (spreadsheet attachment to SW-SEC00045356–357, which is an email with subject line “FedRAMP_Security_Controls_Baseline as of 06282019_1 08272019.xlsx,” August 28, 2019).

⁸⁸ Ms. Pierce indicated in red those controls for which there had been “No program/practice in place,” in yellow the controls for which “Program/Practice may be in place but requires detailed review,” and in green the controls for which there was a “Program/Practice in place.” SW-SEC00045358 (FedRAMP spreadsheet, August 28, 2019), at tab ‘MODERATE kp METRICS’ (cells D7-F8).

⁸⁹ The spreadsheet defines “Family (Column C): Control family designations in alignment with the NIST SP 800-53 organization.” SW-SEC00045358, at tab ‘Key to LMH Baselines’ (cell A14).

controls were rated “No program/practice in place,” including four controls categorized as “Least Privilege.”⁹⁰

65. The assessment further stated that, while the concept of “least privilege” is “included in the Access/Security Guidelines document,” an “audit that this is in place has **never** been performed” (emphasis added).⁹¹ Without an audit in place to confirm whether the principle of least privilege is actually being followed (rather than simply being included in guidelines), my opinion is that an organization cannot be certain about whether access controls are, in fact, “set on a need-to-know / least privilege necessary basis.”⁹²

66. Based on my review of this August 2019 assessment, SolarWinds lacked a policy to enforce least privilege and did not audit compliance with the least privilege principle. Put simply, it appears SolarWinds leaders knew that they did not have a policy in place, nor a way to verify whether the least privilege principle was being adhered to. Therefore, in my opinion, the categorical assertion in the Security Statement that “access controls [...] are [...] set on a need-to-know / least privilege necessary basis,”⁹³ is not justified by the evidence I have reviewed.

67. My review of internal documents also identified another serious access control/least privilege issue, related to the SolarWinds MSP class of products and services. Managed Service Providers (MSPs) provide customers with IT infrastructure and services,

⁹⁰ There were six controls with “LEAST PRIVILEGE” as part of the “Control Name,” (column E) out of which four had been colored in red to indicate “No program/practice in place.” See SW-SEC00045358, at tab ‘MODERATE SUMMARY KP’ (Rows 17-22); at tab ‘MODERATE kp METRICS’ (cells D7-F8).

⁹¹ SW-SEC00045358 (FedRAMP spreadsheet, August 28, 2019), at tab ‘MODERATE SUMMARY KP’ (Rows 17 and 19).

⁹² SW-SEC00466120–142 (SolarWinds’ Security Statement), at 132.

⁹³ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132.

sometimes necessitating access to customers' network environment, either on-site or in the MSP's data center.⁹⁴

68. According to an internal presentation dated November 2019:

“MSP Support staff has a significant level of **system level access** to both MSPs and MSP customers. The level of access is **excessive** and if abused **poses a significant insider threat**. Currently, a support person has the ability to gain privileged access, connect or run procedures on one or more MSPs and their customer environments.”⁹⁵ [Emphasis added.]

69. The presentation also stated that “Recent incidents have involved support staff and engineering’s inappropriate access to customers environments.”⁹⁶ In other words, this concern was not merely theoretical—actual incidents had already taken place. Another presentation from the same period requests authorization for a “Review of MSP Support’s access to customer systems, in order to reduce the potential of an insider threat.”⁹⁷

⁹⁴ The IT infrastructure and services that a typical MSP offers include network and information system management, remote monitoring, service desk operations, and incident management. *See, e.g.*, CISA, “Protecting Against Cyber Threats to Managed Service Providers and their Customers,” May 11, 2022, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-131a>. *See also* Kumbakara, Narayanan, “Managed IT Services: The Role of IT Standards,” *Information Management & Computer Security*, Vol. 16, No. 4, July 22, 2008, pp. 336–359.

⁹⁵ SW-SEC00631418–427 (Presentation, “MSP Support Security Improvement,” November 2019), at 419. Emphasis omitted from original.

⁹⁶ SW-SEC00631418–427 (Presentation, “MSP Support Security Improvement,” November 2019), at 419. Emphasis omitted from original.

⁹⁷ My interpretation of the metadata leads me to believe that this presentation was edited by Rani Johnson. SW-SEC00298504–519 at 509 (a slide subtitled “November 2019 [Project] Authorization Requests”).

70. Providing “system level access” (which the presentation pointed out) to people who do not need it is a serious access control issue and a violation of the least privilege principle, an important element of access control best practice. Users with system-level access have complete control over a computer, meaning they can typically read, overwrite, and delete anything on a system; crash the system; remove other users’ accounts; or grant system-level access to other users.⁹⁸ With “system level access to both MSPs and MSP customers,”⁹⁹ the risk—as explicitly laid out in the presentation—a SolarWinds employee could, from the SolarWinds system, perform any of the above actions on a customer system. In my opinion, the slide is correct that this arrangement “poses a significant insider threat.”¹⁰⁰ In other words, a bad actor within SolarWinds (or a hacker who gains access to a SolarWinds user account with such permissions) would be able, for example, to install malware or shut down a customer’s system. This is because, according to the presentation, the software SolarWinds sold gave SolarWinds employees complete control over the computer systems of this class of MSP customers.

71. This incident, related to what SolarWinds described as an “excessive” level of access to customer systems,¹⁰¹ contradicts the Security Statement. “Excessive” access is, by

⁹⁸ See, e.g., NIST Special Publication 800-53 p. 412 (“[P]rivileged account [is] [a] system account with the authorizations of a privileged user.”; “[P]rivileged user [is] [a] user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.” Emphasis removed.); p. 22 (“Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. Privileged roles include key management, account management, database administration, system and network administration, and web administration.”).

⁹⁹ SW-SEC00631418–427 at 419.

¹⁰⁰ SW-SEC00631418–427 at 419. See also, SW-SEC00298504 at 509 (a slide subtitled “November 2019 [Project] Authorization Requests,” which lists “Review of MSP Support’s access to customer systems, in order to reduce the potential of an insider threat.”).

¹⁰¹ SW-SEC00631418–427 at 419.

definition, a violation of the “least privilege” principle.¹⁰² Therefore, allowing an “excessive” level of access to customer assets means that access to these assets was not set on a “need-to-know / least privileged necessary” basis.

72. Having pointed out these problems, the slide suggests that an “Anticipated Outcome” of implementing these security improvements is “Support roles aligned with least privilege”—underscoring SolarWinds’ awareness that the support roles *were not currently aligned* with the least privilege principle.¹⁰³

73. I understand that this problem may have been remediated by April 2020, roughly five months after it was uncovered.¹⁰⁴ In my opinion, this is a potentially catastrophic cybersecurity problem, in addition to constituting a clear violation of the principle of least privilege—and thus, an obvious inconsistency with the Security Statement’s assertion that SolarWinds set access controls on a least privilege basis. Therefore, the Security Statement’s assertions regarding the principle of least privilege, during the time that this was not resolved, were inconsistent with what SolarWinds leadership knew to be occurring.

74. As I describe in **Section IV.B.3.d** in more detail, failing to set access on a least privilege / need-to-know basis exposes the organization to a large number of security risks as a result of accidental or malicious unauthorized access.¹⁰⁵ Potential insider attacks can have dire

¹⁰² As I described above, the Security Statement asserted that SolarWinds’ assets included “customer and end-user assets.” SW-SEC00466120–142 (SolarWinds’ Security Statement) at 129.

¹⁰³ SW-SEC00631418–427 (Presentation, “MSP Support Security Improvement,” November 2019) at 419.

¹⁰⁴ An internal presentation prepared by or presented to the DOIT team in April 2020 marked this project “Complete,” and lists Mr. Brown as one of the DOIT Leads for the project. SW-SEC00356992–7083 (Presentation titled “Major Project Portfolio + Key Initiatives,” April 2020) at 019. (“Key Milestones / Status [-] Complete”; “DOIT Lead – Kellie Pierce, Tim Brown” at the top-left corner of the slide.).

¹⁰⁵ NIST Special Publication 800-53, p. 38 (“The misuse of privileged functions, either intentionally or unintentionally by authorized users or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations.”).

consequences, including destruction of data, deletion of files, or the introduction of malware.

Failure to adhere to the principle of least privilege, giving users more privileges than they need, increases the attack surface (*i.e.*, gives attackers more opportunities to compromise the security of a system).¹⁰⁶

- b. Internal documents contradicted the assertion that role-based access controls were implemented that granted access to resources based on employees' specific job function*

75. In direct contrast with the Security Statement's assertion that SolarWinds implements role-based access control whereby employees are "granted access to certain additional resources based on their specific job function,"¹⁰⁷ internal documents indicate that SolarWinds did not consistently follow this practice.

76. Below I describe two specific events, which senior SolarWinds employees were made aware of, illustrating that broader than necessary access was granted to resources that SolarWinds described as "very sensitive."¹⁰⁸ Although my experience teaches me that the implementation of access controls may not always be perfect, the fact that role-based access

¹⁰⁶ See, e.g., Warsinske et al. (2019) Chapter 5 - Identity and Access Management, p. 511 ("As a top priority, you must protect against the compromise of highly privileged accounts. With sufficient privileges, one can modify log files in a way that is difficult to detect. It may even be possible to alter the 'reality' of the computer system itself by introducing subtle yet nefarious changes into the operating system via so-called rootkits. Once the very foundation of a system's operation comes under an adversary's control, accountability is hard indeed to recover.").

¹⁰⁷ "Role based access controls are implemented for access to information systems. [...] SolarWinds employees are granted a limited set of default permissions to access company resources, such as their email, and the corporate intranet. Employees are granted access to certain additional resources based on their specific job function." SW-SEC00466120-142 (SolarWinds' Security Statement) at 132.

¹⁰⁸ The first event relates to a dataset that Senior Product Manager Andrey Rodushkin described as "very sensitive": "The problem is that new O365 data is very sensitive and it's limited to Superuser access level." SW-SEC00254254-266 at 263. The second incident relates to what Mr. Brown considered to be SolarWinds' "main download site," from which hackers might distribute malware directly to SolarWinds' customers by disguising malware as a legitimate SolarWinds product: "I have made an assumption that this is our main download site since [we] needed to confirm the download site with on internal checksums [sic]. The point they were making was that they could have corrupted one of our downloads. Replacing files or corrupting what was present in our download site." SW-SEC00407702-707 at 702.

controls were not in place in relation to systems and datasets that *SolarWinds itself considered to be so important* (as I explain below) is inconsistent with the categorical assertion of the Security Statement. The Security Statement says categorically that “Employees are granted access to certain additional resources based on their specific job function.”¹⁰⁹

77. Additionally, as I explain below, the problem is not that these two specific circumstances occurred; the problem is that circumstances *of this magnitude* could develop as a result of poor access control practices. In one circumstance (described in **Section IV.B.3.b.i**), developers were using *shared logins* to a *highly privileged account* accessing a *production* dataset—thus violating at least three different assertions from the Security Statement.¹¹⁰ In another event (described in **Section IV.B.3.b.ii**), a SolarWinds downloads repository was created with an *extremely weak* and *publicly exposed* password creating the risk that hackers might *distribute malware directly to SolarWinds customers* by disguising malware as a legitimate SolarWinds product. This arrangement also violated at least three additional assertions from the Security Statement.¹¹¹ The fact that such major events slipped through the cracks is indicative of systemic issues.

¹⁰⁹ SW-SEC00466120–142 (SolarWinds’ Security Statement), at 132.

¹¹⁰ Using shared logins is inconsistent with “We require that authorized users be provisioned with unique account IDs.” Providing unnecessary access to highly privileged accounts is inconsistent with “Role based access controls are implemented for access to information systems.” Developers accessing the production dataset is inconsistent with “SolarWinds maintains separate development and production environments.” SW-SEC00466120–142 (SolarWinds’ Security Statement) at 131-132.

¹¹¹ Using the password “solarwinds123” is inconsistent with the Security Statement’s categorical assertion that SolarWinds “enforce[s] the use complex passwords.” Knowing that a password to a sensitive system was publicly available is inconsistent with the Security Statement’s categorical assertion that “[a]ccess controls to sensitive data in [] databases, systems, and environments [were] set on a need-to-know / least privilege necessary basis.” Knowing that a password was stored in *plaintext format* is inconsistent with the Security Statement’s categorical assertion that SolarWinds had “password best practices.” SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132.

78. Indeed, internal documents suggest that systemic issues were present with regard to identity management and role-based access control. For example, the following four issues taken together are inconsistent with the Security Statement’s assertion that “SolarWinds employees are granted a limited set of default permissions to access company resources, such as their email, and the corporate intranet. Employees are granted access to certain additional resources based on their specific job function. Requests for additional access follow a formal process.”¹¹²

- a. An internal presentation from January 8, 2018 stated that “there is no organization-wide, standardized approach to access management that includes provisioning, changing and de-provisioning users [sic] access to systems that contain personal information.”¹¹³ This internal presentation warned that “[t]he lack of standardized user access management processes that captures [sic] user provisioning (hiring), user changes (transfer) and user de-provisioning (resignation and termination), across the organization create [sic] a loss risk of organizational assets and personal data.”¹¹⁴ Therefore, this presentation highlights that SolarWinds was aware of not only the lack of processes to implement role-based access control (as explicitly asserted by the Security Statement),¹¹⁵ but also of the significant cybersecurity risks the corporation was facing by not having such processes in place.

¹¹² SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132.

¹¹³ SW-SEC00043620–630 (Presentation, “User Access Management – Tool Evaluation and Recommendation,” January 8, 2018) at 621.

¹¹⁴ SW-SEC00043620–630 (Presentation, “User Access Management – Tool Evaluation and Recommendation,” January 8, 2018) at 621.

¹¹⁵ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132.

- b. In September 2018, an internal presentation suggested that SolarWinds’ “Role and Privilege management” program was “[l]imited or non existent [sic].”¹¹⁶ Clearly, a limited or non-existent role and privilege management program is inconsistent with the Security Statement’s assertion that “Role based access controls are implemented for access to information systems.”¹¹⁷
- c. An August 2019 presentation suggested that SolarWinds had an “ad-hoc, inconsistent, or reactive approach” to its authentication and identity management process.¹¹⁸ Again an ad-hoc identity management process is inconsistent with the Security Statement’s assertion that a “formal process” was in place, for any part of authentication and authorization.¹¹⁹
- d. According to Ms. Johnson, as of Q1 2020, SolarWinds’ lack of “authoritative list of everybody” resulted in overlooked SolarWinds users whose “access should have been flagged to either have a renewal or re-approval.”¹²⁰ As Ms. Johnson testified, “the owners of those lists didn’t run their processes properly.”¹²¹ Again,

¹¹⁶ SW-SEC00386134–143 (Presentation, “Information security – Incident review,” September 2018) at 143. (The slide titled “Security Program Status” lists the program “Identity Management – Role and Privilege management” in red font, indicating a status of “Limited or non existent [sic].”)

¹¹⁷ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132.

¹¹⁸ The Security Category “Authentication, Authorization, and Identity Management,” with the Objective “User identity, authentication and authorization are in place and actively monitored across the company”, was assigned a NIST Maturity Level of 1, corresponding to an “ad-hoc, inconsistent, or reactive approach.” SW-SEC00001497–550 (Presentation, “Security & Compliance Program Quarterly Overview,” August 16, 2019) at 505 and 507.

¹¹⁹ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132. (“Employees are granted access to certain additional resources based on their specific job function. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as defined by our security guidelines.”).

¹²⁰ SW-SEC00632171–200 (Q2 2020 Quarterly Risk Review (QRR), May 22, 2020) at 189. *See also*, Investigative Testimony of Rani Johnson - Vol. I Amended, March 17, 2022 (“Johnson Investigative Testimony, Vol. I Amended”) at 117:16-121:25.

¹²¹ Johnson Investigative Testimony, Vol. I Amended at 120:7-8.

overlooked employees and improperly-run user lists, together with the other statements from these internal documents, are inconsistent with the Security Statement's categorical assertions regarding formal role-based access control.

(i) *Developers had "Super User" access to billing data*

79. In November 2019, Mr. Brown was made aware that certain developers had unnecessary access to a dataset that a SolarWinds Senior Product Manager described as a "very sensitive" dataset.¹²² As I described above, although access controls may not always be perfect, the fact that role-based access controls were not in place in relation to a dataset that SolarWinds employees considered to be "very sensitive" is inconsistent with the categorical statement of the Security Statement that "Employees are granted access [...] based on their specific job function."^{123,124}

80. Internal documents between November 2019 and July 2020 indicate that Tim Brown accepted that some SolarWinds employees had broader access than necessitated by their job function, and thus that the role-based access principle (and, concomitantly, the least privilege principle) had been violated.¹²⁵ Specifically, a summary of outstanding risk acceptance forms¹²⁶

¹²² SW-SEC00254254–266 at 263. (Andrey Rodushkin: "The problem is that new O365 data is very sensitive and it's limited to SuperUser access level. And this level has read&write [sic] permissions.").

¹²³ SW-SEC00466120–142 (SolarWinds' Security Statement), at 132. ("SolarWinds employees are granted a limited set of default permissions [...] Employees are granted access to certain additional resources based on their specific job function.")

¹²⁴ Because this issue also relates to SolarWinds' methods of developing software, I further elaborate on these problems in Section IV.D. SW-SEC00168778–779 & SW-SEC00168780. ("Developers [of the BizApps Billing DB] have write access to production Backup data as a part of their permission set. They are using the API's just to pull data for usage billing but those (3) API's have write permissions which are not used or needed.").

¹²⁵ Mr. Brown had reviewed and approved the risk on November 18, 2019. SW-SEC00168780, at tab '7.13.2020 Review,' cell M9 (under "Compensating Control" column). *See also*, SW-SEC00254254–266 (email chain November 14–18, 2019).

¹²⁶ As previously explained, the Risk Acceptance Form was a process that identified SolarWinds' risks and vulnerabilities. Through this process, SolarWinds defined a timeline for risks to be remediated that needed to be

dated July 13, 2020 stated that “[d]evelopers have write access [...] which are not used or needed.”¹²⁷

81. The “write access” described in this incident report relates to the type of permission granted to certain employees. Various types of permissions exist, each of which carry different levels of privilege—and thus, different levels of risk if the privilege is abused. For example, “read” permission allows a person only to *view* the data without altering it, so it is considered low risk in terms of data integrity.¹²⁸ On the other hand, a person with “write” permission can *alter* (and in many cases, delete) the data, potentially leading to loss, corruption, or modification of important information, making that permission level higher risk and therefore more privileged.¹²⁹ Providing someone with write privileges who should be given only lower privileges violates the principle of least privilege. As I describe below, this can lead to the accidental or malicious alteration or deletion of important data, and makes it more difficult to prevent, detect, and remediate malicious behavior. Additionally, expert attackers often make it a

agreed upon by the Vice-President of Security or higher-level executives. *See, e.g.*, SW-SEC00168009–017 (Presentation, “Risk Acceptance Form (RAF) Process,” August 2020), at 011. (“The Risk Acceptance Form (RAF) is to be used in instances where the risk is likely to exist for more than 1 month and/or if risk actualized, the event would trigger our security incident response process. The RAF must be approved by the SolarWinds Executive (Vice President or higher) responsible for the asset or service accepting the risk.”). *See also* Quitugua Investigative Testimony, Vol. I, at 196:17-25. (“Q [...] What is the risk acceptance form process? A That’s a process [...] by which risks are identified. They can be remediated [...] in a [sic] agreed upon timeline that [...] get submitted through this risk acceptance form for review and approval by the VP of security and for acceptance of risk or a denial of risk.”).

¹²⁷ SW-SEC00168780, at tab ‘7.13.2020 Review,’ cell C9 (under “Summary of Request” column).

¹²⁸ NIST Special Publication 800-53, p. 75. (“Restricting privileged user or role authorizations to read-only helps to limit the potential damage to organizations that could be initiated by such users or roles, such as deleting audit records to cover up malicious activity.”).

¹²⁹ NIST Special Publication 800-53 p. 88. (“Verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations (i.e., write permissions or privileges) prior to accepting such data [...] [t]o prevent unauthorized individuals and systems from making information transfers to protected systems[.]”).

special point to gain unauthorized access to highly privileged accounts, as a means of compromising system security protections including access controls.¹³⁰

82. The email chain from November 2019 states that the developers had “Super User” access, with which a user “has read&write [sic] permissions,” “can make edits, changes, etc.” and “could potentially do actions that would have financial impact.”^{131, 132} The access in question related to production data, which was apparently captured for usage billing purposes.¹³³ In my experience, it is highly unusual for developers to have *write* access to production data for usage billing purposes, or indeed for any reason. SolarWinds employees openly discussed that providing this level of access to a “very sensitive” data to the developers was not “the best short term solution,” “will always [be] challenge[d],” and “should probably be under SOX control.”¹³⁴

83. Providing people who do not need it with read and write access (and potentially “Super User” access) is a serious access control issue. For example, if developers had read/write

¹³⁰ See, e.g., CISA, “Technical Approaches to Uncovering and Remediating Malicious Activity,” September 24, 2020, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-245a>. (“Service accounts are privileged accounts dedicated to certain services to perform activities related to the service or application without being tied to a single domain user. Given that services tend to be privileged accounts and thereby have administrative privileges, they are often a target for attackers aiming to obtain credentials.”).

¹³¹ SW-SEC00254254–266. (“The problem is that new O365 data is very sensitive and it’s limited to SuperUser access level. And this level has read&write permissions.”; “This is a request we will always challenge as with SuperUser access you can make edits, changes, etc.”; “Because they are going to have Super User access and could potentially do actions that would have financial impact this should probably be under SOX control.”; “BizApps has a couple of shared logins with Superuser access to Production Backup data in order to pull data for billing (using 2 different API’s)[.]”)

¹³² In my reading, it is unclear whether the developers also have system-level Super User access, in addition to read and write access, or if “Super User” is being used in an application-specific context.

¹³³ SW-SEC00168780, at tab ‘7.13.2020 Review,’ cell C9 (under “Summary of Request” column). (“Developers [of the BizApps Billing DB] have write access to production Backup data as a part of their permission set. They are using the API’s just to pull data for usage billing but those (3) API’s have write permissions which are not used or needed.”)

¹³⁴ SW-SEC00254254–266 (“The problem is that new O365 data is very sensitive and it’s limited to SuperUser access level. And this level has read&write permissions.”; “If we can stick to read only access that would be the best short term [sic] solution.”; “This is a request we will always challenge as with SuperUser access you can make edits, changes, etc.”; “Because they are going to have Super User access and could potentially do actions that would have financial impact this should probably be under SOX control.”).

access to usage data used for billing, they could potentially modify the underlying usage to change the amounts that people were charged, or to pass a customer's information on to its competitors.

84. Importantly, the existence of this incident was indicative of a deeper issue than a one-off error. As I elaborate further in **Sections IV.C and IV.D** below, by accessing this “very sensitive” dataset, the developers violated several further security best practices (and the corresponding assertions in the Security Statement): the developers should never have had access to the production environment in the first place,¹³⁵ and yet they accessed the data through shared logins,¹³⁶ which is considered poor practice.¹³⁷ The fact that a problem of this magnitude occurred—developers using *shared logins* to a *highly privileged account* accessing a *production* dataset—should have alerted SolarWinds' leadership that practices were not in place to ensure that the Security Statement's assertions were consistently implemented across the organization. At a minimum, this incident was inconsistent with the following assertions from the Security Statement:

¹³⁵ See NIST Special Publication 800-53, pp. 98, 103. (“Establishing separate baseline configurations for development, testing, and operational environments protects systems from unplanned or unexpected events related to development and testing activities. [...] Limiting privileges to change system components with respect to operational systems is necessary because changes to a system component may have far-reaching effects on mission and business processes supported by the system.”).

¹³⁶ SW-SEC00254254–266 at 265. (“[The developers] are currently using a shared login [...] of a different SolarWinds employee. This is definitely a security incident and needs to stop.”).

¹³⁷ See NIST Special Publication 800-53, pp. 22, 132. (“Before permitting the use of shared or group accounts, organizations consider the increased risk due to the lack of accountability with such accounts. [...] Control: Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.”).

- a. Providing unnecessary access to highly privileged accounts is inconsistent with “Role based access controls are implemented for access to information systems.”¹³⁸
- b. Using shared logins is inconsistent with “We require that authorized users be provisioned with unique account IDs.”¹³⁹ (I elaborate further in **Section IV.C** below.)
- c. Developers accessing the production dataset is inconsistent with “SolarWinds maintains separate development and production environments.”¹⁴⁰ (I elaborate further in **Section IV.D** below.)

85. Furthermore, although Mr. Brown was made aware of this access control violation in November 2019 and agreed that it should be remediated by January 31, 2020, the violation remained unaddressed until at least July 13, 2020—over five months beyond the date by which Mr. Brown agreed the risk must be remediated.¹⁴¹ Meeting notes from June 8, 2020,¹⁴² and from July 13, 2020 indicate that Mr. Brown was made aware that the risk had not yet been mitigated.¹⁴³ In other words, Mr. Brown knew that SolarWinds continued to violate the role-based access controls described in the Security Statement; yet, the language of the Security Statement did not change.

¹³⁸ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132.

¹³⁹ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132.

¹⁴⁰ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 131.

¹⁴¹ SW-SEC00168778–779 & SW-SEC00168780, at tab ‘7.13.2020 Review,’ cells F9, K9 and L9. (“11/18/19: Risk reviewed by and accepted by Tim Brown.” and “Risk Acceptance Expiration (date by which risk will be remediated). [...] 1/31/2020”).

¹⁴² The RAF noted that an email was sent to the responsible employee for a status update. SW-SEC00168778–779 & SW-SEC00168780 at tab ‘7.13.2020 Review,’ cell M9. (“6/8/20: Email sent to Rick for update”).

¹⁴³ SW-SEC00168778–779 at 778.

(ii) *Write access credentials for a SolarWinds download server were posted publicly*

86. Internal emails between November 2019 and December 2020 discussed that a password that allowed users to “upload anything to downloads.solarwinds.com” was accidentally made publicly available.^{144,145} As I understand the situation, members of the public had write access to a system SolarWinds used to distribute software to customers. As I describe below, SolarWinds was aware that this represented a potentially serious security vulnerability for SolarWinds and its customers. Clearly, if *the public* had access to this system, then role-based access controls were not in place (as the public had no “specific job function” at SolarWinds that would necessitate access) and access to this system was not determined on a least privilege necessary basis (as the public should not have had this privilege). Therefore, industry norms of software distribution and access control were not adhered to.¹⁴⁶

87. The functionalities to which this leaked password provided access represented a potentially serious security vulnerability for SolarWinds and its customers. In short, by publicly disclosing the credentials to SolarWinds’ FTP¹⁴⁷ site from which customers normally

¹⁴⁴ SW-SEC00407702–707 at 702, 704. *See also*, SW-SEC00001476–484 at 484 (“We have received an inquiry about hard-coded credentials, which are publicly available and allows attacker to upload files to our FTP download server”); SW-SEC00001464 (an email sent by PSIRT to InfoSec team on November 19, 2019). (“Hi Team, I have found a public Github repo which is leaking ftp credential belongs to SolarWinds. [...] Username: solarwindsnet Password: solarwinds123 [...] Via this any hacker could upload malicious exe and update it with release SolarWinds product.”); SW-SEC00001476–484 at 483 (“This was a previous password for the main Akamai Upload Account. It was still in an active state.”).

¹⁴⁵ I note that this issue was caught by an “external researcher,” not by SolarWinds, either as a result of an internal access control audit or a configuration management alert. SW-SEC00407702–707 at 704.

¹⁴⁶ *See* NIST Special Publication 800-53, pp. 36, 38. (“Organizations employ least privilege for specific duties and systems. The principle of least privilege is also applied to system processes, ensuring that the processes have access to systems and operate at privilege levels no higher than necessary to accomplish organizational missions or business functions. [...] Policies and procedures for granting equivalent status of employees to individuals include a need-to-know, citizenship, and the relationship to the organization.”).

¹⁴⁷ An FTP (file transfer protocol) is a standard communication tool to establish a secure connection between devices to efficiently transmit data over the internet. FTPs are typically used to exchange large files and to enhance

downloaded SolarWinds content, anyone on the internet could *upload* malicious software into this repository. SolarWinds' customers could then *download* these malicious files, while thinking that they were downloading legitimate SolarWinds materials.¹⁴⁸ The severity of the issue was recognized by Tomas Sejna (Senior Security Engineer), who stated that this publicly available password “allows attacker [sic] to upload files to our FTP download server.”¹⁴⁹ Mr. Brown agreed, stating that:¹⁵⁰

“With that credential they could upload anything to downloads.solarwinds.com . [...] In their POC [proof of concept] they uploaded a file to the site. I have made an assumption that this is our main download site since [we] needed to confirm the download site with on internal checksums [sic]. The point they were making was that they could have corrupted one of our downloads. Replacing files or corrupting what was present in our download site.”

88. As of November 19, 2019, SolarWinds employees were not able to ascertain whether “the compromised login information was not abused in the past,”¹⁵¹ and they estimated

the security of a file exchange. SolarWinds, “What Is FTP Server?,” <https://www.solarwinds.com/resources/it-glossary/ftp-server>.

¹⁴⁸ SW-SEC00407702–707 at 704. (“Via this any hacker could upload malicious exe [*i.e.*, an executable file] and update it with release SolarWinds product.”); SW-SEC00001476–484 at 477. (“Per information from release management, they are working on double checking that no files on Akamai has [sic] been modified. Because we are using signed executables, it is *very* [sic] unlikely but we are double cheking [sic] it anyway. Once this process is finished, this security incident can be closed.”).

¹⁴⁹ SW-SEC00001476–484 at 484.

¹⁵⁰ SW-SEC00407702–707 at 702.

¹⁵¹ SW-SEC00001476–484 at 480.

that it would take until the end of November to check all of the close to 6,000 files that may have been compromised.¹⁵² Indeed, it can be difficult, once improper access has been granted to a repository, to *ever* ascertain whether files have been tampered with. Clever attackers have many tools at their disposal to cover their tracks, such as modifying the contents of a file in a malicious way while changing the file to conceal the tampering.¹⁵³

89. To make matters worse, the password that had been leaked was “solarwinds123,” which Mr. Brown and Mr. Quitugua both described as “a very weak password,”¹⁵⁴ and Mr. Quitugua also testified that it lacked “complexity.”¹⁵⁵ Of course, in addition to the access control violation described above, this incident also represented a violation of the assertion in the Security Statement requiring the use of “complex” passwords, as I describe in **Section IV.C** below in more detail.

90. SolarWinds employees also discussed that it “might make sense moving forward” to create a special account “with account rights limited only to this specific action.”¹⁵⁶ In other words, the account for which the password has been leaked had not been set up according to the least privilege principle and access control best practices, because it allowed a broader scope of actions than was necessary. This incident therefore represented multiple independent violations

¹⁵² SW-SEC00001476–484 at 476. (“We have 5707 files to be compared. We will provide an update by End of November on our progress.”).

¹⁵³ See e.g., Warsinske et al. (2019) Chapter 5 - Identity and Access Management, p. 511. (“With sufficient privileges, one can modify log files in a way that is difficult to detect. It may even be possible to alter the “reality” of the computer system itself by introducing subtle yet nefarious changes into the operating system via so-called rootkits.” Emphasis removed.).

¹⁵⁴ SW-SEC00407702–707 at 702 (Mr. Brown admitted that the solarwinds123 incident “did take place and a very weak password existed to access that environment.”); Quitugua Investigative Testimony, Vol. II, at 361:14-16 (“Would you agree that that is a very weak password? A Yes.”).

¹⁵⁵ Quitugua Investigative Testimony, Vol. II, at 361:20-21. (“A You know, numbers in sequence, all lower case, no complexity, uses common names.”).

¹⁵⁶ SW-SEC00001476–484 at 483. (“It might make sense moving forward to use special account only for MIB uploads with account rights limited only to this specific action.”)

of the access control best practices to which the Security Statement claimed to adhere: *even if* the password had not been as weak as it was, and *even if* the credentials had not been made publicly available, the practice of maintaining an account that allowed unauthorized uploads violated the principle of least privilege and unnecessarily increased the attack surface on SolarWinds and on its customers.

91. Therefore, rather than a one-time accident of an intern setting a weak password,¹⁵⁷ this incident illustrates more pervasive problems at SolarWinds as a whole, related to both access control and user authentication. The fact that even an intern working on “his bachelor thesis” was able to *publicly expose an extremely weak password* to a system that *allows any hacker to upload malicious files that SolarWinds customers could subsequently download* is, in and of itself, indicative of a systemic issue. The problem is not that this specific incident occurred; the problem is that an incident *of this magnitude* could develop as a result of poor access control practices. According to Mr. Brown, *SolarWinds effectively made it possible for hackers to distribute malware directly to SolarWinds customers by disguising malware as a legitimate SolarWinds product.*¹⁵⁸ As remediation, an internal SolarWinds document from December 2020 stated that “There will be special training introduce[d] to ensure something like that does not

¹⁵⁷ SW-SEC00407702–707 at 704. (“Engineering intern was working on MIB [Management Information Base] upload functionality improvements. He used the code as a project for his bachelor thesis. He accidentally uploaded it to Github including configuration file that contained login and password for publishing files to Akamai. [...] There was no bad intention, it happened accidentally and was also related to juniority of the intern who did not think about it properly before the publishing.”).

¹⁵⁸ SW-SEC00407702–707 at 702. (“With that credential they could upload anything to downloads.solarwinds.com [...] In their POC [proof of concept] they uploaded a file to the site. I have made an assumption that this is our main download site since [we] needed to confirm the download site with on internal checksums [sic]. The point they were making was that they could have corrupted one of our downloads. Replacing files or corrupting what was present in our download site.”).

happen anymore.”¹⁵⁹ The fact that such training—and other, technical controls preventing such an issue—were not in place before reflects a systemic issue at SolarWinds.

92. Mr. Brown’s December 2020 email to his colleagues describing this issue indicates recognition of this being a serious issue. He wrote: “This was managed and resolved quickly but *it did take place* [emphasis added] and a very weak password existed to access” the environment that “could have corrupted one of our downloads.”¹⁶⁰ Indeed, the fact that this vulnerability was quickly remediated does not mitigate the fact that this fundamental cybersecurity weakness, suggestive to me of systemic problems, should not have existed in the first place if SolarWinds had followed the security practices asserted in the Security Statement.

93. In my opinion, this incident indicates such fundamental problems that it should have alerted SolarWinds leadership that there were pervasive flaws in the company’s access control practices that were inconsistent with assertions in the Security Statement. At a minimum, this incident was inconsistent with several assertions from the Security Statement, as I discuss below.

- a. Mr. Brown and Mr. Quitugua both admitted that the password “solarwinds123” was *not a complex* password¹⁶¹ and not a one-time occurrence.¹⁶² This incident is

¹⁵⁹ SW-SEC00407702–707 at 704.

¹⁶⁰ SW-SEC00407702–707 at 702.

¹⁶¹ SW-SEC00407702–707 at 702 (Mr. Brown admitted that the solarwinds123 incident “did take place and a very weak password existed to access that environment.”); and Quitugua Investigative Testimony, Vol. II, at 361:14-16 (“Would you agree that that is a very weak password? A Yes.”; at 361:20-21 (“A You know, numbers in sequence, all lower case, no complexity, uses common names.”).

¹⁶² Quitugua Investigative Testimony, Vol. II, at 362:7-15 (“Q Are you aware of solarwinds123 being used as a password in other parts of the organization? A [...]. There may have been the possibility that in the lab environments, passwords such as, you know, weak passwords that were in use.”); Brown Deposition at 120:14-15 (“A I’m not saying that [...] the password policy was followed a hundred percent of the time.”).

therefore inconsistent with the Security Statement’s categorical assertion that SolarWinds “enforce[s] the use complex passwords.”¹⁶³

- b. Mr. Brown acknowledged the fact that the password to a sensitive system (which, according to Mr. Brown, would potentially allow attackers to “corrupt one of our downloads”)¹⁶⁴ was *publicly available*. This is inconsistent with the Security Statement’s categorical assertion that “[a]ccess controls to sensitive data in [] databases, systems, and environments [were] set on a need-to-know / least privilege necessary basis.”¹⁶⁵
- c. Mr. Brown acknowledged that the password was available in the public file in *plaintext format*.¹⁶⁶ This is inconsistent with the Security Statement’s categorical assertion that SolarWinds had “password best practices.”¹⁶⁷ (I describe this in more detail in **Section IV.C.3** below.)

c. *Internal documents contradicted the assertion that processes and procedures are in place to address employees who are voluntarily or involuntarily terminated*

94. In direct contradiction with the Security Statement’s assertion that “[p]rocesses and procedures are in place to address employees who are voluntarily or involuntarily

¹⁶³ SW-SEC00466120–142 (SolarWinds’ Security Statement), at 132. (“Our password policy covers all applicable information systems, applications, and databases. Our password best practices enforce the use of complex passwords that include both alpha and numeric characters, which are deployed to protect against unauthorized use of passwords.”).

¹⁶⁴ SW-SEC00407702–707 at 702. (I described this in more detail in **Section IV.B.**)

¹⁶⁵ SW-SEC00466120–142 (SolarWinds’ Security Statement), at 132.

¹⁶⁶ SW-SEC00407702–707 at 704. Mr. Brown’s email included the following root cause analysis finding: “Engineering intern was working on MIB upload functionality improvements. He used the code as a project for his bachelor thesis. He accidentally uploaded it to Github including configuration file that contained login and password for publishing files to Akamai.”

¹⁶⁷ SW-SEC00466120–142 (SolarWinds’ Security Statement), at 132.

terminated,”¹⁶⁸ an internal SolarWinds presentation from January 8, 2018 stated that “system users who have changed roles or left the company may still have access to critical data.”¹⁶⁹ The presentation also warned that such “lack of standardized user access management processes [...] create a loss risk of organizational assets and personal data.”¹⁷⁰ Therefore, this presentation highlights that SolarWinds was aware of not only the lack of consistent processes to address deprovisioning credentials for terminated employees, but also of the significant cybersecurity risks the corporation was running by not having such processes in place.

95. The same was reflected in an internal security incident notification email from January 4, 2018 stating that “ex members of staff” had access to a “Google Document” containing elevated access credentials, “along with instructions on how to use this information.”¹⁷¹ The notification also stated that the “Google Doc could be accessed from a home broadband connection via a private browser window and thus was accessible without authentication via the Internet.”¹⁷² This email warned that, “if exploited[, this] would allow access to all data” in one of SolarWinds’ products.¹⁷³ Indeed, SolarWinds was internally aware

¹⁶⁸ SW-SEC00466120–142 (SolarWinds’ Security Statement), at 132.

¹⁶⁹ SW-SEC00043620–630 (Presentation, “User Access Management – Tool Evaluation and Recommendation,” January 8, 2018), at 621.

¹⁷⁰ SW-SEC00043620–630 (Presentation, “User Access Management – Tool Evaluation and Recommendation,” January 8, 2018), at 621.

¹⁷¹ SW-SEC00427486–488 (Email from Chris Day to Rene Van Steenberg and Oliver Wood, January 4, 2018), at 487–488. (“A Google Document, tied to the gfilabs.com G-Suite contains a URL, username and password to grant ‘god like access’ to RMM US Reseller Dashboard, along with instructions on how to use this information. The file hounddog key is also required (described in the document) and this is also in a shared folder. [...] The document and hounddog key files have had their access restricted to members of the gfilabs.com G -Suite however this includes ex members of staff.”)

¹⁷² SW-SEC00427486–488 (Email from Chris Day to Rene Van Steenberg and Oliver Wood, January 4, 2018), at 488.

¹⁷³ SW-SEC00427486–488 (Email from Chris Day to Rene Van Steenberg and Oliver Wood, January 4, 2018), at 487. (“Elevated RMM [Remote Monitoring & Management] access credentials exposed in publicly available Google Doc and if exploited would allow access to all data in RMM.”)

that these access credentials were not being “stored in an internal, secure environment following best practices.”¹⁷⁴ The email also suggests that this was not an isolated incident but a repeated issue, and that senior SolarWinds employees were aware of its severity: “This is a — they f’d up, twice now — I’m hard pressed to even understand why they need a gfilabs G-suite account.... but at minimum they can’t store any confidential information there.”¹⁷⁵

96. Similarly, an October 2019 internal presentation,¹⁷⁶ as explained by Ms. Johnson’s Investigative Testimony, stated that in some cases there were delays in removing access from ex-employees: “there were a few instances where team members waited beyond that day period to remove access to things that were non-material systems, but nevertheless, the discipline was not yet in place.”¹⁷⁷

97. Additionally, the Q2 2020 Quarterly Risk Review presentation described that 18 individuals had been identified as “active” who were in fact “inactive contractors and/or vendors.”¹⁷⁸ In her Investigative Testimony, Ms. Johnson explained that “[t]hose team members either left before their period of assigned access terminated and did not have that recorded, or

¹⁷⁴ SW-SEC00427486–488 (Email from Chris Day to Rene Van Steenberg and Oliver Wood, January 4, 2018), at 488. (“We need to be more autocratic on this — all files containing sensitive information (username/pwd etc) need to be immediately removed off the g suite account. That information should be stored in an internal, secure environment following best practices (e.g. secret server etc).”)

¹⁷⁵ SW-SEC00427486–488 (Email from Chris Day to Rene Van Steenberg and Oliver Wood, January 4, 2018), at 488.

¹⁷⁶ SW-SEC00151415–421 (Presentation, “SOC 2 Executive Update – DOIT: Security & Compliance Program Office”) at 420.

¹⁷⁷ Johnson Investigative Testimony, Vol. I Amended at 90:6-14. (“[A]s team members were leaving, there was a -- we used to call it a spam email sent to system owners as a compensating control to ensure that any system that didn’t have that integration with AD would result in access removal. [...] [T]here were a few instances where team members waited beyond that day period to remove access to things that were non-material systems, but nevertheless, the discipline was not yet in place[.]”)

¹⁷⁸ SW-SEC00632171–200 (Q2 2020 Quarterly Risk Review (QRR), May 22, 2020), at 189. (“The Service Desk team identified 18 additional individuals [sic] who were identified as active, however were inactive contractors and/or vendors.”)

extended beyond that period -- they either left before or they had access in a period beyond when they were deemed to leave.”¹⁷⁹ Although Ms. Johnson testified that, after noticing this error, SolarWinds ascertained that none of these 18 individuals did access the systems after they left SolarWinds,¹⁸⁰ this apparent outcome is irrelevant. The outcome that a security breach did not materialize—or at least, was not determined by SolarWinds to have materialized—does not negate the fact that these individuals had access to SolarWinds systems after their contracts were terminated, contrary to the Security Statement.

98. This issue is illustrated in a SARF (System Access Request Form) document from October 2018. As Mr. Bliss explained in his deposition, SolarWinds used a manual process, called SARF, to “establish access rights for individuals based on their role as they were both onboarded, as they changed roles in the company, as they were offboarded.”¹⁸¹ This SARF document from October 30, 2018 shows an ad-hoc process. As shown below, SolarWinds

¹⁷⁹ Johnson Investigative Testimony, Vol. I Amended, at 121:9-121:20. (“Q And the last bullet point down, says ‘The service desk team identified 18 [...] additional individuals who are identified as active, however were inactive contractors and/or vendors.’ Do you see that? A Yes. Q Can you explain to me what that related to? A Those team members either left before their period of assigned access terminated and did not have that recorded, or extended beyond that period -- they either left before or they had access in a period beyond when they were deemed to leave.”).

¹⁸⁰ Johnson Investigative Testimony, Vol. I Amended, at 121:20-121:25. (“And so those specific ones -- and that’s part of the reason they’re highlighted in yellow -- all of -- that whole collection were audited to make sure that there was no inappropriate access to any systems beyond that period and it was confirmed that no one -- none of them did access the systems afterwards.”)

¹⁸¹ Deposition of Jason Bliss (30(b)(6)), *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, October 16, 2024 (“Bliss Deposition (30(b)(6))”) at 118:17-22. (“A. We had a process that utilized what’s called a SARF, S-A-R-F, form that would establish access rights for individuals based on their role as they were both onboarded, as they changed roles in the company, as they were offboarded.”). *See also* Brown Deposition at 204:21-205:3. (“A. We had a manual process to onboard and give appropriate access rights to people called S-A-R-F. And what that process was, was a process where somebody joined a company, went to HR. HR would send an email to IT with an appropriate rule and then those rules would say onboard this person in this way.”).

employees discussed that, because they do not know the termination date of a “temp” (*i.e.*, a temporary worker), they decided to provide his account with a one-year expiration date.¹⁸²

“Can you also clarify for a new start that is a temp, what length of time should I make their AD before it expires? Was there a date given to when the temp will finish? [...]

No, none. [...]

Then there should be one. Did you ask the recruiter/HR [...]

There is no end date, like I used to have [...]

do for 1 year so [...]

Will do, cheers. [...]

99. In my opinion, the above examples show that senior SolarWinds employees were aware that, contrary to the assertions in the Security Statement, SolarWinds did not consistently implement the “[p]rocesses and procedures [...] to address employees who are voluntarily or involuntarily terminated.”¹⁸³ As I described above, these internal documents also indicate that senior SolarWinds employees were aware of the significant cybersecurity risks to which the corporation was exposed by not having such processes in place.

d. A failure to follow the access controls that the Security Statement described exposed the organization to company-wide cybersecurity risks

100. In **Sections IV.B.3.a-c**, I provided many examples of instances in which the practices that SolarWinds discussed in internal documents were inconsistent with the categorical

¹⁸² SW-SEC-SDNY_00050922 at 922.

¹⁸³ SW-SEC00466120–142 (SolarWinds’ Security Statement), at 132.

assertions made in the Security Statement regarding the company's access control. In this section, I explain why these inconsistencies were grave from a cybersecurity perspective. Specifically, as I explain below, a failure to follow the access controls that the Security Statement described exposed the organization to company-wide cybersecurity risks.

101. As noted above, no organization has perfect cybersecurity and that any organization diligently assessing its cybersecurity will uncover, from time to time, some issues needing to be addressed. However, the access control problems that I have pointed out above, reflected in SolarWinds' internal documents and testimony, do not constitute the kind of routine minor problems that a company would encounter if it followed the security best practices and industry norms in the manner described in the Security Statement. In my opinion, the discrepancies between SolarWinds' internal documents and the Security Statement within the area of access control are reflective of significant deviations from industry norms, with potential company-wide impact.

102. In the aggregate, the wide range of access control failures I described in the preceding sections not only constituted a departure from the assertions in the Security Statement, but also exposed both SolarWinds and its customers to elevated cybersecurity risks.

103. To help conceptualize the elevated cybersecurity risks to which SolarWinds' practices exposed the company, it is helpful to think of the company as a house. There are various methods to reduce the risk of burglary to one's house, including locking the doors, not keeping the key in obvious places such as under the door mat, and enabling an alarm. The more of these practices a homeowner undertakes, the less likely it is that the house will be broken into. Similarly, there are various methods to reduce the risk of a successful cyberattack, including the access control practices that SolarWinds asserted in the Security Statement it was doing:

assigning access control on a role based / least privilege / need-to-know basis, ensuring that terminated employees no longer have access, and following a formal process for additional access.¹⁸⁴ The more gaps an organization has in following these practices, the more likely it is that a hacker will successfully attack the organization. As I described in **Section III.A**, cybersecurity's fundamental defense-in-depth principle states that organizations should apply multiple security layers to ensure that vulnerabilities not remediated by one countermeasure are addressed by another.¹⁸⁵

104. The Security Statement asserted that SolarWinds (1) set access controls based on a need-to-know or least privilege basis; (2) limit employees' access to those resources that were required to perform their roles; or (3) revoke the access of those employees who left the organization. These practices are standard practices within the cybersecurity industry with respect to access control. However, the internal documents I described above indicate that SolarWinds did not, as they categorically asserted in the Security Statement, follow these practices. Each of these failures would be problematic on their own. Combined, they are akin to, at the same time, not enabling the alarm and not locking the front door. These flawed practices, together, significantly decreased the level of protection.

105. Industry bodies, including NIST, ISO, SANS, CERT/CC, and CISA, agree that not following the principle of least privilege (and thus, not following commonly accepted access

¹⁸⁴ SW-SEC00466120–142 (SolarWinds' Security Statement) at 132. ("Role based access controls are implemented for access to information systems. Processes and procedures are in place to address employees who are voluntarily or involuntarily terminated. Access controls to sensitive data in our databases, systems, and environments are set on a need-to-know / least privilege necessary basis. [...] SolarWinds employees are granted a limited set of default permissions to access company resources, such as their email, and the corporate intranet. Employees are granted access to certain additional resources based on their specific job function. Requests for additional access follow a formal process [...].")

¹⁸⁵ NIST, "Glossary – 'Defense-in-Depth'," https://csrc.nist.gov/glossary/term/defense_in_depth.

control practices), can expose the organization to several types of risks.¹⁸⁶ As I describe below, these risks can include: (1) increased exposure to external attacks; (2) increased risk of insider threats; (3) increased difficulty with preventing, detecting, and responding to cyberattacks; and (4) other operational risks. In addition, it can lead to regulatory non-compliance.¹⁸⁷

106. First, excessive privileges increase exposure to cyberattacks by expanding the attack surface.¹⁸⁸ Attackers look for privileged accounts as a primary target, and when many accounts have elevated access, the chances of successful exploitation rise.¹⁸⁹ In addition to raising the *likelihood* of a successful attack, over-privileged users and applications also increase

¹⁸⁶ NIST Special Publication 800-53, p. 38. (“The misuse of privileged functions, either intentionally or unintentionally by authorized users or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Logging and analyzing the use of privileged functions is one way to [...] help mitigate the risk from insider threats and the advanced persistent threat.”); ISO/IEC 27001:2013(E), A.9.2.3. (“The allocation and use of privileged access rights shall be restricted and controlled” with the objective “to prevent unauthorized access to systems and services.”); Shackleford, Dave and Arick Goomanovsky, “Mitigate Access Risk by Enforcing Least Privilege in Cloud Infrastructure,” SANS, September 16, 2020, <https://www.sans.org/webcasts/mitigate-access-risk-enforcing-privilege-cloud-infrastructure-116290/> (“[D]evelopers tend to grant broad entitlements, resulting in ‘permission creep’ which is very difficult to eliminate in production. As many as 90% of these permissions are unused, excessive, and a tremendous risk to the environment.”); Miller, Sarah, “Separation of Duties and Least Privilege (Part 15 of 20: CERT Best Practices to Mitigate Insider Threats Series),” SEI, July 26, 2017 <https://insights.sei.cmu.edu/blog/separation-of-duties-and-least-privilege-part-15-of-20-cert-best-practices-to-mitigate-insider-threats-series/> (“In addition to protecting against malicious attacks, separation of duties and least privilege also assists in mitigating unintentional insider threats.”); CISA, “Technical Approaches to Uncovering and Remediating Malicious Activity,” September 24, 2020, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-245a> (“Decrease a threat actor’s ability to access key network resources by implementing the principle of least privilege.”).

¹⁸⁷ See, e.g., Sarbanes-Oxley Act § 404. Management Assessment of Internal Controls. See also, GDPR Article 32, at Article 32: Security of Processing; ISO/IEC 27001:2013(E), A.18.1.3. (“Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislative, regulatory, contractual and business requirements.”).

¹⁸⁸ NIST Special Publication 800-53, p. 282. (“Attack surface reduction is a means of reducing risk to organizations by giving attackers less opportunity to exploit weaknesses or deficiencies [...] Attack surface reduction includes [...] applying the principles of least privilege and least functionality[.]”).

¹⁸⁹ See, e.g., Miller, Sarah, “Separation of Duties and Least Privilege (Part 15 of 20: CERT Best Practices to Mitigate Insider Threats Series),” SEI, July 26, 2017 <https://insights.sei.cmu.edu/blog/separation-of-duties-and-least-privilege-part-15-of-20-cert-best-practices-to-mitigate-insider-threats-series/> (“If no single employee has the privileges necessary to access and leak the ‘secret sauce,’ then there is no single point of failure if employees are targeted by a social engineering campaign.”).

the potential impact of a breach. For instance, if attackers compromise an account with administrative privileges, they can use it to install malware, access databases, or exfiltrate data.

107. Second, excessive privileges also increase the risk of accidental or intentional insider threats.¹⁹⁰ If a user has more privileges than necessary, they could inadvertently access and modify critical systems or data, leading to security breaches, data loss, or unauthorized changes.¹⁹¹ Malicious insiders with elevated privileges can cause severe damage by accessing or stealing sensitive information that they wouldn't normally have access to.¹⁹²

108. Third, excessive privileges may also make it more difficult to prevent, detect, and respond to cyberattacks (both external and internal).¹⁹³ Prevention may be more difficult

¹⁹⁰ See, e.g., NIST Special Publication 800-53, p. 342. (“Privileged users have access to more sensitive information, including security-related information, than the general user population. Access to such information means that privileged users can potentially do greater damage to systems and organizations than non-privileged users. Therefore, implementing additional monitoring on privileged users helps to ensure that organizations can identify malicious activity at the earliest possible time and take appropriate actions.”).

¹⁹¹ NIST Special Publication 800-53, p. 38. (“The misuse of privileged functions, either intentionally or unintentionally by authorized users or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Logging and analyzing the use of privileged functions is one way to [...] help mitigate the risk from insider threats and the advanced persistent threat.”).

¹⁹² Shackleford, Dave and Arick Goomanovsky, “Mitigate Access Risk by Enforcing Least Privilege in Cloud Infrastructure,” SANS, September 16, 2020, <https://www.sans.org/webcasts/mitigate-access-risk-enforcing-privilege-cloud-infrastructure-116290/> (“[D]evelopers tend to grant broad entitlements, resulting in ‘permission creep’ which is very difficult to eliminate in production. As many as 90% of these permissions are unused, excessive, and a tremendous risk to the environment.”); Miller, Sarah, “Separation of Duties and Least Privilege (Part 15 of 20: CERT Best Practices to Mitigate Insider Threats Series),” SEI, July 26, 2017 <https://insights.sei.cmu.edu/blog/separation-of-duties-and-least-privilege-part-15-of-20-cert-best-practices-to-mitigate-insider-threats-series/> (“In addition to protecting against malicious attacks, separation of duties and least privilege also assists in mitigating unintentional insider threats.”).

¹⁹³ See NIST Special Publication 800-53, p. 38. (“The misuse of privileged functions, either intentionally or unintentionally by authorized users or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations.”); CISA, “Technical Approaches to Uncovering and Remediating Malicious Activity,” September 24, 2020, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-245a> (“Decrease a threat actor’s ability to access key network resources by implementing the principle of least privilege.”).

because, as discussed above, excessive privileges increase the organization's attack surface.¹⁹⁴

With broader access, attackers—whether external or internal—have more entry points and systems to target, heightening the likelihood of a successful breach.¹⁹⁵ Detection may be slower or more difficult because, if many employees have excessive privileges, it becomes challenging to discern whether specific actions taken were authorized or malicious.¹⁹⁶ Remediation may be more difficult because a slower detection time can allow a security incident to become more severe and widespread, which can make it harder to identify and respond to the source of the breach.¹⁹⁷

109. Fourth, excessive privileges can expose the organization to other operational risks because they can lead to accidental changes, system outages, data corruption, and other errors or disruptions in normal operations. For example, users with too many privileges might make

¹⁹⁴ NIST Special Publication 800-53, p. 282. (“Attack surface reduction is a means of reducing risk to organizations by giving attackers less opportunity to exploit weaknesses or deficiencies [...] Attack surface reduction includes [...] applying the principles of least privilege and least functionality[.]”).

¹⁹⁵ NIST Special Publication 800-53, p. 282. (“Attack surface reduction includes implementing the concept of layered defenses, applying the principles of least privilege and least functionality, [...] reducing entry points available to unauthorized users, reducing the amount of code that executes, and eliminating application programming interfaces (APIs) that are vulnerable to attacks.”).

¹⁹⁶ *See, e.g.*, NIST Special Publication 800-53, p. 262. (“Applying the principle of least privilege limits the scope of the component's actions, which has two desirable effects: the security impact of a failure, corruption, or misuse of the component will have a minimized security impact, and the security analysis of the component will be simplified.”); Warsinske et al. (2019) Chapter 5 - Identity and Access Management, p. 511. (“As a top priority, you must protect against the compromise of highly privileged accounts. With sufficient privileges, one can modify log files in a way that is difficult to detect. It may even be possible to alter the “reality” of the computer system itself by introducing subtle yet nefarious changes into the operating system via so-called rootkits. Once the very foundation of a system's operation comes under an adversary's control, accountability is hard indeed to recover.”).

¹⁹⁷ *See, e.g.*, ISO/IEC 27001:2013(E), A.16.1.2. (“Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses. [...] Information security events shall be reported through appropriate management channels as quickly as possible.”); CISA, “Technical Approaches to Uncovering and Remediating Malicious Activity,” September 24, 2020, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-245a> (“If an attacker (or malware) gains access to a remote user's computer, steals authentication data (login/password), hijacks an active remote administration session, or successfully attacks a vulnerability in the remote administration tool's software, the attacker (or malware) will gain unrestricted control of the enterprise network environment. Attackers can use compromised hosts as a relay server for reverse connections, which could enable them to connect to these remote administration tools from anywhere.”).

unintended changes to critical systems, configuration settings, or sensitive data.¹⁹⁸ This can lead to downtime, system failures, or corrupted data, costing the company both time and money.¹⁹⁹ SolarWinds was aware of this threat: for example, a January 2018 internal presentation warned that the “lack of standardized user access management processes [...] across the organization create a loss risk of organizational assets and personal data.”²⁰⁰

110. Finally, excessive privileges can lead to regulatory non-compliance, resulting in fines and penalties. Many industry regulations, such as GDPR and SOX, mandate strict access controls and least privilege enforcement.²⁰¹ Failure to comply with these regulations can result in fines, penalties, legal liability, and reputational damage. Non-compliance with the principle of least privilege might expose sensitive customer data or personal information unnecessarily, leading to breaches that could trigger legal and regulatory actions against the company.²⁰²

¹⁹⁸ See NIST Special Publication 800-53, p. 38. (“The misuse of privileged functions, either intentionally or unintentionally by authorized users or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Logging and analyzing the use of privileged functions is one way to [...] help mitigate the risk from insider threats and the advanced persistent threat.”).

¹⁹⁹ See NIST, *NIST Special Publication 1800-25: Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Event*, December 2020, pp. ii, 8. (“Ransomware, destructive malware, insider threats, and even honest user mistakes present ongoing threats to organizations. Organizations’ data, such as database records, system files, configurations, user files, applications, and customer data, are all potential targets of data corruption, modification, and destruction. [...] Types of vulnerabilities we consider in relation to these threats are: [...] poor access control[.] Finally, we consider the potential impact on an organization from a [data integrity] event: systems incapacitated[,], modification/deletion of organization’s assets[, and] negative impact on the organization’s reputation.”).

²⁰⁰ SW-SEC00043620–630 (Presentation, “User Access Management – Tool Evaluation and Recommendation,” January 8, 2018) at 621.

²⁰¹ See, e.g., Sarbanes-Oxley Act § 404. Management Assessment of Internal Controls. See also, GDPR Article 32, at Article 32: Security of Processing; ISO/IEC 27001:2013(E), A.18.1.3 (“Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislative, regulatory, contractual and business requirements.”)

²⁰² See, e.g., SANS Institute, *Implementing Least Privilege at Your Enterprise*, July 5, 2003, at “Least Privilege and Standards” section (“There are many examples of organizations that have been found negligent and held liable in courts of law, because they have failed to follow the [least privilege and due diligence] best practices of the industry.”).

C. SolarWinds Internal Documentation and Testimony Show That SolarWinds Did Not Consistently Follow the Assertions in the Security Statement Regarding Passwords and User Authentication

111. As I explain below, my opinion is that the practices that SolarWinds described in internal documents were inconsistent, from a cybersecurity perspective, with certain password and user authentication related assertions made in the Security Statement. SolarWinds did not, in the manner that was represented in the Security Statement, enforce the use of unique account IDs or conform to password best practices. By failing to apply the user authentication controls described in the Security Statement in a consistent manner, SolarWinds amplified the company's cybersecurity risks.

112. In this section, I first provide an overview of the importance of passwords and authentication controls within the context of cybersecurity (**Section IV.C.1**). Second, I present potentially verifiable (or falsifiable) assertions made by SolarWinds in its public Security Statement concerning passwords and authentication controls (**Section IV.C.2**). Third, I interpret both the Security Statement and SolarWinds' internal documents describing passwords and user authentication in the context of the well-accepted industry norms that were available during the Relevant Period. As I described in **Section IV.A**, these industry norms present the context of the Security Statement. Based on my first-hand experience with these industry norms, as well as my interpretation of the guidance from industry bodies described below, I find that internal communications within SolarWinds revealed employee awareness of the company's inconsistent implementation of these authentication controls, and that SolarWinds failed to meet widely accepted industry norms (**Section IV.C.3**).

1. *Introduction to passwords and user authentication*

113. Because authenticating the identity of a user is important for ensuring that only authorized users can access information, there are several commonly accepted industry norms related to authentication management. For example, if an organization decides to use passwords as a method of authentication, then, during the Relevant Period, it was generally recommended to use a password of at least eight characters.²⁰³ It is always important to ensure, regardless of the length of the password, that the password is complex and not easily guessable (such as the word “password,” or the user’s username).²⁰⁴

114. There are also commonly accepted industry norms regarding how to securely store user passwords. Password storage is important because even the longest and most complex password can be stolen if it is stored in “plaintext” form (*i.e.*, without any encryption, such that a bad actor can easily read and copy the password).²⁰⁵ The problem, as OWASP explains,²⁰⁶ is that “[s]toring a plaintext password in a configuration file allows anyone who can read the file access to the password-protected resource.”²⁰⁷

²⁰³ See, e.g., NIST, *NIST Special Publication 800-63B: Digital Identity Guidelines*, June 2017 (“NIST Special Publication 800-63B”) at Section 5 (“Memorized secrets SHALL be at least 8 characters in length if chosen by the subscriber.”).

²⁰⁴ Warsinske et al. (2019) Chapter 5 - Identity and Access Management, p. 498 (“Many common password guidelines require passwords to be the following: Complex, Long, Different, and Nonobvious.”); NIST Special Publication 800-63B at Section 5 (“Memorized secrets SHALL be at least 8 characters in length if chosen by the subscriber. [...] values known to be commonly-used, expected, or compromised [...] include, but is not limited to: • Passwords obtained from previous breach corpuses. • Dictionary words. • Repetitive or sequential characters (e.g. ‘aaaaaa’, ‘1234abcd’). • Context-specific words, such as the name of the service, the username, and derivatives thereof.” (emphasis in original)).

²⁰⁵ See CWE, “CWE-256: Unprotected Storage of Credentials,” *available on* December 20, 2020, <http://web.archive.org/web/20201220094745/https://cwe.mitre.org/data/definitions/256.html>.

²⁰⁶ As I described in **Section III.A**, OWASP is “a nonprofit foundation that works to improve the security of software.” OWASP, “About the OWASP Foundation,” <https://owasp.org/about>.

²⁰⁷ OWASP, “Password Plaintext Storage,” *available on* October 27, 2020, https://web.archive.org/web/20201027103906/https://owasp.org/www-community/vulnerabilities/Password_Plaintext_Storage.

2. *The SolarWinds Security Statement made assertions about passwords and user authentication*

115. The Security Statement stated the following with respect to passwords:

- a. “We require that authorized users be provisioned with **unique account IDs**.”²⁰⁸
- b. “**Our password policy** covers all applicable information systems, applications, and databases. **Our password best practices enforce the use of complex passwords** that include both alpha and numeric characters, which are deployed to protect against unauthorized use of passwords.”²⁰⁹

3. *SolarWinds failed to follow the password and user authentication practices asserted in the Security Statement*

116. Despite the above public assertions, internal SolarWinds’ communications throughout the Relevant Period and testimony indicate that the statements described above were inaccurate from the perspective of a trained cybersecurity professional.

- a. *Internal documents contradicted the assertion that SolarWinds requires that authorized users be provisioned with unique account IDs*

117. In contradiction with the public statement that SolarWinds “require[s] that authorized users be provisioned with unique account IDs,”²¹⁰ I have found several examples describing the use of shared accounts during the Relevant Period. To explain why the inconsistencies between the Security Statement and SolarWinds’ *de facto* practices were

²⁰⁸ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132. Emphasis added.

²⁰⁹ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132. Emphasis added.

²¹⁰ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132.

particularly grave from a cybersecurity perspective, in this section I show that SolarWinds’ practices represented a significant deviation from industry norms that have been specifically developed by the cybersecurity community to minimize the risk of cyberattacks.

118. As reflected in NIST’s recommendations, it is a well-accepted cybersecurity norm that each user has unique login credentials.²¹¹ The sharing of accounts among multiple employees is generally poor practice, and it increases security risks to the organization. One reason is that the more users are aware of a password, the more likely it is that—accidentally or intentionally—the password gets exposed to a bad actor. Another reason is that the use of shared accounts interferes with the auditing process.²¹² If login credentials are shared, it becomes much more difficult to identify the person responsible for a particular action taken via that account.

119. Internal documents suggest that SolarWinds employees were aware that the company did not consistently enforce the use of unique account IDs. For example, an internal document from March 2018 noted the use of “shared accounts throughout internal and external applications.”²¹³ Mr. Quitugua testified that this reference to shared accounts referred to purpose-built service accounts, that is, accounts that should have been exclusively used for the purposes they were created, but instead were being used by “multiple people” for “whatever business

²¹¹ NIST Special Publication 800-53, p. 132. (At IA-2 Identification and Authorization, “Control: Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users. [...] [Discussion:] Since processes execute on behalf of groups and roles, organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity.”).

²¹² I described this in more detail in **Section IV.B**. *See also* NIST Special Publication 800-53, pp. 22, 132 (“Before permitting the use of shared or group accounts, organizations consider the increased risk due to the lack of accountability with such accounts. [...] Control: Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.”).

²¹³ SW-SEC00012265–275 (email with presentation attached, March 15, 2018) at 268.

use.”^{214,215} Clearly, if *shared* accounts are used *throughout* internal and external applications, then SolarWinds was not enforcing the use of *unique* account IDs, as suggested by the Security Statement.²¹⁶

120. Similarly, in April 2018, an email circulating the results of an internal audit stated that “[s]hared SQL legacy account login credentials [were] used” for three business units.²¹⁷ SQL is a programming language used to query, update, and organize data.²¹⁸ Again, if account credentials are *shared*, then they are not *unique* to each user, as stated by the Security Statement.

121. Importantly, based on these documents, not only were SolarWinds employees aware of the violation of the industry norm (reflected in the Security Statement) of not sharing account credentials; they were also aware of maintaining conditions that posed a security risk to

²¹⁴ Quitugua Investigative Testimony, Vol. II at 289:20-292:6. (“Q [...] So early 2018, and you were saying that the use of shared accounts was an issue that you identified in this presentation. I’m just wondering why was it that shared accounts were being used in time period? A [...] What we found was that these service accounts, which were purpose built to run processes, were also being used by, you know, users, and they also knew the credentials, right. So that case, we considered those accounts shared accounts, accounts that users should not have access to had access to credentials. So although there was a legitimate business use case for the use of the service account, multiple people had access to that service account[.] [...] Q And [...] you made a statement that users were using the service account. Who are you referring to when you say ‘users’? A So the administrators of the application, right, if you’re developing the application, they may have had access to that same service account, and using that account for whatever business use.”).

²¹⁵ I understand that the purpose of these shared accounts may have included “processing data, moving data between the web frontend into the database,” and to “authenticate [users] into the database.” Quitugua Investigative Testimony, Vol. II at 290:25-291:9. (“Q [...] So the purpose built service accounts, what was the [...] proper business use for those [accounts]? A So things like, you know, processing data, moving data between the web frontend into the database, right. In order to authenticate into the database, a service account would be used to authenticate to the database a trusted account used to authenticate to the database.”).

²¹⁶ The Security Statement refers not to shared accounts but to “unique account IDs.” My interpretation of this sentence is that, in accordance with cybersecurity norms, shared accounts were not to be used. *See* SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132.

²¹⁷ SW-SEC00043080–084 (Email chain with subject line “Please follow up on Risk/Compensating Controls,” April 13, 2018) at 081-083.

²¹⁸ SQL stands for Structured Query Language. *See* NIST, “SQL,” *available on* October 20, 2020, <https://web.archive.org/web/20201020184906/https://csrc.nist.gov/glossary/term/SQL>. *See also*, Mucci, Tim, “What Is Structured Query Language (SQL)?,” IBM, May 31, 2024, <https://www.ibm.com/think/topics/structured-query-language>.

the company. First, the internal audit rated the risk level of this incident as “High.”²¹⁹ Second, when asked to provide additional details, a SolarWinds engineer responded, “my understanding is these are old [SQL] accounts that are shared among multiple [databases]/websites and **pose a security risk**” (emphasis added).²²⁰

122. Additionally, in November 2019, SolarWinds employees raised an alarm about developers “using a shared login currently of a different SolarWinds employee.”²²¹ Again, a “shared login” is the opposite of “unique account IDs,” as stated by the Security Statement. And, again, SolarWinds employees were aware of the security risks to which this practice had exposed the company. They discussed that this practice was “not secure,”²²² “definitely a security incident and needs to stop,”²²³ and includes a “risk of data leak when employee leaves.”²²⁴

123. Moreover, as I described in **Section IV.B** above, the shared login discussed in this November 2019 email chain related to developers having higher than necessary access (“Super User” “write” access).²²⁵ Furthermore, as I will describe in **Section IV.D** below, this access was

²¹⁹ SW-SEC00043080–084 (Email chain with subject line “Please follow up on Risk/Compensating Controls,” April 13, 2018) at 081-083.

²²⁰ SW-SEC00043080–084 (Email chain with subject line “Please follow up on Risk/Compensating Controls,” April 13, 2018) at 080.

²²¹ SW-SEC00254254–266 at 265. (From Sean O’Shea: “They are currently using a shared login currently of a different SolarWinds employee. This is definitely a security incident and needs to stop.”). *See also*, SW-SEC00254254–266 at 261. (From Sean O’Shea: “Also right now they are using a shared login so giving them their own read only login would be better than the current solution of a shared login.”).

²²² SW-SEC00254254–266 at 258. (From Sean O’Shea: “When challenged it turns out they are all using a common login currently which is also not secure.”).

²²³ SW-SEC00254254–266 at 265. (From Sean O’Shea: “They are currently using a shared login currently of a different SolarWinds employee. This is definitely a security incident and needs to stop.”).

²²⁴ SW-SEC00254254–266 at 258. (From Sean O’Shea, quoting the BizApps team: “Our BizApps (Finance) team is constantly working on improving our billing system and they need to have Backup accounts per each developer to reduce risk of data leak when employee leaves.”).

²²⁵ SW-SEC00254254–266. *See Section IV.B* for more detailed discussion.

to a production dataset to which the developers never should have had access in the first place.²²⁶

Having *shared logins* to a *highly privileged account* accessing a *production* dataset violates industry norms (and the corresponding Security Statement assertions) related to user authentication, access control, and SDL. I will discuss the significance of this access issue more fully in **Section IV.D** below related to SolarWinds' secure development lifecycle.

b. Internal documents contradicted the assertion that SolarWinds conformed to password best practices

124. The Security Statement asserted the following:

“Our password policy covers all applicable information systems, applications, and databases. **Our password best practices enforce the use of complex passwords** that include both alpha and numeric characters, which are deployed to protect against unauthorized use of passwords.”^{227,228}

125. As a cybersecurity professional, I interpret the above assertion as stating that SolarWinds comported with industry norms related to password best practices. However, my review of internal documents found that SolarWinds employees were aware that they did not

²²⁶ SW-SEC00254254–266. See **Section IV.D** for more detailed discussion.

²²⁷ SW-SEC00466120–142 (SolarWinds' Security Statement) at 132. Emphasis added.

²²⁸ A more detailed version of the Security Statement, shared with SolarWinds' customers upon request, provided the requirements of a “complex password.” See SW-SEC00010210–229 (email and Detailed SolarWinds Security Statement, May 2018) at 210, 224. (“Our password policy covers all applicable information systems, applications, and databases. Our password best practices enforce the use complex passwords that include both alpha and numeric characters which are deployed to protect against unauthorized use of passwords. Users on the SolarWinds domain must create strong passwords that meet the following complexity requirements: Passwords cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters. • Passwords must be at least 8 characters in length. • Passwords must contain characters from three of the following four categories: • English uppercase characters (A through Z). • English lowercase characters (a through z). • Base 10 digits (0 through 9). • Non-alphabetic characters (for example, !, \$, #, %).”).

consistently conform to industry best practices as they relate to passwords. Below I present two examples, both of which show that SolarWinds did not have systems in place to ensure that the assertion in the Security Statement was correct.

(i) *Storing plaintext or hard-coded passwords in configuration files violates common industry norms*

126. One commonly accepted industry norm is that storing plaintext or hard-coded passwords in configuration files violates best practices.²²⁹ A hard-coded plaintext password in programming refers to embedding a password directly into the source code or configuration file, making it fixed and readable to anyone who has access to the file. Hard-coded sensitive data such as credentials are a well-known vulnerability. If hard-coded passwords are used, this makes it easier for malicious users to gain access to the account in question.²³⁰ The problem, as OWASP explains, is that “[s]toring a plaintext password in a configuration file allows anyone who can read the file access to the password-protected resource.”²³¹

127. According to OWASP, storing passwords in insecure ways is a leading cause of security breaches.²³² SolarWinds was aware of the severity of this problem, with Mr. Brown

²²⁹ CWE, “CWE-256: Unprotected Storage of Credentials,” *available on* December 20, 2020, <http://web.archive.org/web/20201220094745/https://cwe.mitre.org/data/definitions/256.html>. (“Password management issues occur when a password is stored in plaintext in an application’s properties or configuration file. Storing a plaintext password in a configuration file allows anyone who can read the file access to the password-protected resource.”). *See also*, CWE, “CWE-798: Use of Hard-coded Credentials,” *available on* October 21, 2019, <https://web.archive.org/web/20191021162254/https://cwe.mitre.org/data/definitions/798.html>. (“Hard-coded credentials typically create a significant hole that allows an attacker to bypass the authentication that has been configured by the software administrator.”).

²³⁰ CWE, “CWE-798: Use of Hard-coded Credentials,” *available on* October 21, 2019, <https://web.archive.org/web/20191021162254/https://cwe.mitre.org/data/definitions/798.html>.

²³¹ OWASP, “Password Plaintext Storage,” *available on* October 27, 2020, https://web.archive.org/web/20201027103906/https://owasp.org/www-community/vulnerabilities/Password_Plaintext_Storage.

²³² OWASP ranked “Broken Authentication” as the 2nd most critical risk in its Top 10 list of Web Application Security Risks between at least 2017 and 2020, noting that “Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or

stating in a September 2019 interview that “[p]asswords that were stored in the wrong way” are responsible for a large number of successful cybersecurity attacks.²³³

128. Despite this well-known vulnerability, the evidence I have examined indicates that SolarWinds employees did include hard-coded plaintext passwords in configuration files. An internal assessment circulated on April 13, 2018 stated that “[l]ogin account credentials are stored in plain text in configuration files” and “[p]assword[s] are stored in plain text on the public web servers in the web [] configuration file and in the system registry of the machine.”²³⁴ Similarly, a November 2019 SolarWinds email chain discussed hard-coded credentials (specifically, the password “solarwinds123”): “We have received an inquiry about hard-coded credentials, which are publicly available and allows attacker to upload files to our FTP download server.”²³⁵

129. These examples are reflected in the findings of Kellie Pierce’s 2019 internal assessment, where she stated that “No known policy/practice” was in place with respect to the organization ensuring that “unencrypted static authenticators are not embedded in applications or access scripts.”²³⁶ The simple translation of the term “unencrypted static authenticators” is hard-

session tokens”. OWASP, “OWASP Top 10 Security Risks,” *available on* January 17, 2020, <https://web.archive.org/web/20200117090941/https://owasp.org/www-project-top-ten/>.

²³³ See, e.g., Johnson, O’Ryan, “SolarWinds Security Exec Timothy Brown: MSPs ‘Top Of My Risk Level’,” CRN, *available on* September 06, 2019, <https://web.archive.org/web/20210126084205/https://www.crn.com/solarwinds-security-exec-timothy-brown-mmps-top-of-my-risk-level-/2>. (“Enterprises that get breached. That was their choice. It seriously was. It was 100 percent their choice. If you look at the attacks that have been successful, most of them have been silly mistakes. Passwords that were stored in the wrong way.”).

²³⁴ The document also states, “SQL DB passwords are not encrypted within the configuration file;” and “Passwords are not encrypted in web configuration files.” SW-SEC00043080–084 (Email chain with subject line “Please follow up on Risk/Compensating Controls,” April 13, 2018), at 082.

²³⁵ SW-SEC00001476–484 at 484.

²³⁶ SW-SEC00045358 (FedRAMP spreadsheet, August 28, 2019) at tab ‘MODERATE SUMMARY KP,’ row 152, ID “IA-5(7)” (under column “Kellie’s Comments/Notes” and value: “6/28 KP: No known policy/practice”; and

coded plaintext passwords. Simply put, Ms. Pierce’s note from June 28, 2019 stated that SolarWinds did not systematically ensure that employees conform to the industry best practice of not including hard-coded plaintext credentials in configuration files.

(ii) *Failing to enforce the use of complex passwords violates common industry norms*

130. Another commonly accepted industry norm, explicitly described in the Security Statement, is the use of complex passwords. As NIST explains, if a password is weak—in other words, short or based on common patterns (like “password” or “solarwinds123”)—attackers can easily guess it through brute-force or dictionary attacks.²³⁷ As I explained in one of my books, in some cases, “dedicated password ‘cracker’ hardware can decipher up to 100 million passwords a second.”²³⁸ It is therefore not surprising that obtaining passwords and user credentials is one of the most vulnerable targets for attackers: according to a data breach investigation report, in 2016, “81% of hacking-related breaches leveraged either stolen and/or weak passwords.”²³⁹

131. To protect the organization against such attacks, the ISO 27001 standard requires that password management systems “shall ensure quality passwords.”²⁴⁰ Without strong

under column “NIST Control Description” and value: “The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.”).

²³⁷ NIST Special Publication 800-63B, p. 67. (“Passwords that are too short yield to brute force attacks and dictionary attacks using words and commonly chosen passwords.”).

²³⁸ See, e.g., Warsinske et al. (2019) Chapter 5 - Identity and Access Management, p. 497. (“Passwords may be guessed, either directly (because an attacker knows something about the user or the system that influences the choice of the password) or via the use of special attack software. The science of guessing passwords has advanced to the point that dedicated password ‘cracker’ hardware can decipher up to 100 million passwords a second in some cases.”).

²³⁹ Verizon, *2017 Data Breach Investigations Report 10th Edition*, 2017, pp. 3, 69-70. See also, Warsinske et al. (2019) Chapter 5 - Identity and Access Management, p. 497. (“Passwords are by far the most commonly used authentication mechanism. They are just about the weakest, too.”).

²⁴⁰ ISO/IEC 27001:2013(E), A.9.4.3.

passwords supporting authorized user authentication,²⁴¹ organizations are at risk of data breaches which, as NIST describes, can “compromise[] corporate information including emails, employee records, financial records, and customer data” and “cause a significant loss to a company’s reputation, business operations, and bottom line.”²⁴²

132. Despite this well-known vulnerability, the evidence I have examined indicates that senior SolarWinds employees were aware that SolarWinds failed to implement this industry norm in the manner described in the Security Statement. As I described in more detail in **Section IV.B**, internal emails between November 2019 and December 2020 discussed that the password “solarwinds123” was used in a system.²⁴³ Both Mr. Brown and Mr. Quitugua described the password “solarwinds123” as “a very weak password,”²⁴⁴ and Mr. Quitugua also testified that it lacked “complexity.”²⁴⁵

133. Importantly, according to both Mr. Brown and Mr. Quitugua, the use of such a weak password was likely not a one-time occurrence: Mr. Quitugua acknowledged that “There may have been a possibility that in the lab environments [...] weak passwords” such as

²⁴¹ See CISA, *Capacity Enhancement Guide: Implementing Strong Authentication*, October 8, 2020, p. 1.

²⁴² NIST, *NIST Special Publication 1800-11A: Data Integrity, Recovering from Ransomware and Other Destructive Events*, September 2020, pp. ii, 1.

²⁴³ SW-SEC00407702–707 at 702-704; SW-SEC00001464 (an email sent by PSIRT to InfoSec team on November 19, 2019). (“Hi Team, I have found a public Github repo which is leaking ftp credential belongs to SolarWinds. [...] Username: solarwindsnet Password: solarwinds123 [...] Via this any hacker could upload malicious exe and update it with release Solar Winds product.”).

²⁴⁴ SW-SEC00407702–707 at 702 (Mr. Brown admitted that the solarwinds123 incident “did take place and a very weak password existed to access that environment.”); Quitugua Investigative Testimony, Vol. II at 360:16-361:25. (“Would you agree that that is a very weak password? A Yes.”).

²⁴⁵ Quitugua Investigative Testimony, Vol. II, at 360:16-361:25. (“A You know, numbers in sequence, all lower case, no complexity, uses common names.”).

“solarwinds123” were in use;²⁴⁶ and Mr. Brown acknowledged that SolarWinds’ “password policy was [not] followed a hundred percent of the time.”²⁴⁷ Mr. Brown’s and Mr. Quitugua’s admissions regarding SolarWinds’ lax password policy enforcement are in line with Kellie Pierce’s 2019 internal assessment, where she stated that “minimum password complexity” related requirements “should be in place or remediation plan in place.”²⁴⁸ I interpret this to mean that Ms. Pierce was not able to firmly ascertain whether the password complexity policy was enforced.

134. Simply put, Mr. Brown’s, Mr. Quitugua’s, and Ms. Pierce’s statements taken together depicted a substantially less secure password control environment than the Security Statement’s categorical assertion that SolarWinds “enforce[s] the use complex passwords” on “all applicable information systems, applications, and databases.”²⁴⁹ As they all admitted, SolarWinds did not have a system in place to ensure that the assertion in the Security Statement was correct.²⁵⁰

²⁴⁶ Quitugua Investigative Testimony, Vol. II, at 362:1-25. (“Q Are you aware of solarwinds123 being used as a password in other parts of the organization? A [...]. There may have been the possibility that in the lab environments, passwords such as, you know, weak passwords that were in use.”).

²⁴⁷ Brown Deposition at 120:14-15. (“A I’m not saying that [...] the password policy was followed a hundred percent of the time.”).

²⁴⁸ SW-SEC00045358 (FedRAMP spreadsheet, August 28, 2019), at tab ‘MODERATE SUMMARY KP,’ row 147, ID “IA-5(1)” (under column “Kellie’s Comments/Notes” and value: “6/27 KP: Requirement in Access/Security policy - should be in place or remediation plan in place”).

²⁴⁹ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132.

²⁵⁰ I note that Kellie Pierce’s 2019 internal assessment stated, with respect to the control requiring the organization to develop an “identification and authentication policy,” that such a policy “Does not exist per my knowledge.” However, I have seen a document that Mr. Bliss describes as a “documented outline of general user access management [...] requirements.” As the document states and Mr. Bliss explains, this purported policy applies only to “financially significant” systems, not “**all** applicable information systems, applications, and databases,” as stated by the Security Statement. Bliss Deposition (30(b)(6)) at 149:17-21 (“A. So this is a documented outline of general user access management and, in particular, requirements to certain of our systems that are financially significant and prescribing password complexity, among other things. [...] Q Okay. Is this meant to apply to the entire organization at SolarWinds [...]? A. No”); SW-SEC00223527–532 at 527 (“The purpose of this document is to outline the User Access Management (UAM) and Segregation of Duties (SOD) processes for SolarWinds. [...] This policy is

c. SolarWinds' internal user authentication practices were inconsistent with its public representations in the Security Statement

135. Based on my experience in evaluating the cybersecurity practices of large organizations, my review of SolarWinds' internal documentation, communications, and testimony, and considering the language of the SolarWinds Security Statement, I conclude that the security of SolarWinds' user authentication practices depicted in the company's internal discussions did not match several of the very broad, categorical, and unqualified assertions in the Security Statement.

136. As noted above, no organization has perfect cybersecurity and that any organization diligently assessing its cybersecurity will uncover, from time to time, some issues needing to be addressed. However, the password problems that I have pointed out above, reflected in the SolarWinds internal documents and testimony, do not constitute the kind of routine minor problems that a company would encounter if it followed the security best practices and industry norms in the manner described in the Security Statement. In my opinion, the discrepancies between SolarWinds' internal documents and Security Statement within the area of user authentication are reflective of significant deviations of industry norms, with potential company-wide impact, and in some cases an impact on the security of its customers as well.

applicable to all users of SolarWinds' production financial systems, databases and applications. [...] The Company maintains password requirements for all financially significant systems"). *See also*, SW-SEC00045358 (FedRAMP spreadsheet, August 28, 2019), at tab 'MODERATE SUMMARY KP,' row 134, ID "IA-1" (under column "Kellie's Comments/Notes" and value: "6/27 KP: Does not exist per my knowledge"). SW-SEC00466120–142 (SolarWinds' Security Statement) at 132. Emphasis added.

D. SolarWinds’ Internal Documentation and Testimony Show That, Contrary to the Security Statement, SolarWinds Did Not Consistently Follow “Standard Security Practices” in Its Secure Development Lifecycle

137. Based on my experience in evaluating the cybersecurity practices of large organizations, my review of SolarWinds’ internal documentation, communications, and testimony, and considering the language of the SolarWinds Security Statement, I conclude that the practices SolarWinds described in internal documents were inconsistent, from a cybersecurity perspective, with certain assertions made in the Security Statement related to software development. As I describe below, SolarWinds did not, in the manner that was represented in the Security Statement, enforce the separation of the production environment from the development environment, or enforce standard security practices throughout the software development process.

138. In this section, I first provide an overview of secure development lifecycles within the context of cybersecurity (**Section IV.D.1**). Second, I present potentially verifiable (or falsifiable) assertions SolarWinds made in its public Security Statement concerning developing software under a secure development lifecycle, including performing commonly accepted security tests (**Section IV.D.2**). Third, I interpret both the Security Statement and SolarWinds’ internal documents describing the development of software under a secure development lifecycle in the context of the well-accepted industry norms that were available during the Relevant Period. As I described in **Section IV.A**, these industry norms present the context of the Security Statement. Based on my first-hand experience with these industry norms, as well as my interpretation of the guidance from industry bodies described below, I find that internal communications within SolarWinds revealed employee awareness of the company’s inconsistent implementation of the secure development processes asserted by the Security Statement. By

failing to apply the software development security processes described in the Security Statement in a consistent manner, SolarWinds failed to adhere to industry norms and amplified the cybersecurity risks of the company and many of its customers (**Section IV.D.3**).

1. Introduction to secure development lifecycle and security testing

139. As I describe below, the Security Statement asserted that SolarWinds followed a “secure development lifecycle,” with a “defined methodology for developing secure software.”²⁵¹ Based on my experience, I interpret these phrases to assert that SolarWinds used a software development lifecycle with a special emphasis on security.²⁵²

140. A secure development lifecycle would typically integrate security best practices into each phase of software development, aiming to identify and mitigate vulnerabilities early before malicious actors can exploit them.²⁵³ Such an approach is designed to prevent security flaws and vulnerabilities, which can lead to potential data breaches and require costly fixes.²⁵⁴

²⁵¹ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132. (“We follow a defined methodology for developing secure software that is designed to increase the resiliency and trustworthiness of our products. Our products are deployed on an iterative, rapid release development lifecycle. Security and security testing are implemented throughout the entire software development methodology.”).

²⁵² The Security Statement appears to have used the terms “secure development lifecycle” and “Software Development Lifecycle” interchangeably. I understand that Mr. Brown considered there to be no difference between these two terms. Brown Deposition, at 130:8-19. (“Q. Is there any difference between secure development lifecycle as it is used here and the term software development lifecycle as it is used in the heading in your mind? A. No. Q. Do you understand that Mr. Colquitt’s initiative in 2018 was titled secure development lifecycle? A. I am. Q. So -- and that initiative was not put into place until sometime after SolarWinds’ security statement was posted to its public facing website, correct? A. Correct.”).

²⁵³ See, e.g., Microsoft, “What Are the Microsoft SDL Practices?,” available on January 09, 2019, <https://web.archive.org/web/20190109013652/https://www.microsoft.com/en-us/securityengineering/sdl/practices>.

²⁵⁴ See, e.g., Microsoft, “What Are the Microsoft SDL Practices?,” available on January 09, 2019, <https://web.archive.org/web/20190109013652/https://www.microsoft.com/en-us/securityengineering/sdl/practices>.

141. While efforts to create secure software have been ongoing for decades,²⁵⁵ Microsoft’s introduction of the “Security Development Lifecycle” (SDL) in the early 2000s was a significant step forward.²⁵⁶ The SDL presented a formal process and methodology for building security into every stage of software development.²⁵⁷ Many companies have incorporated similar secure development lifecycle steps into their software development process to help increase the security, reliability, and business integrity of their products, including Cisco, Adobe, and SAP.²⁵⁸

142. During the Relevant Period, a secure development lifecycle—as described by, for example, OWASP—generally included security practices in the areas described below.²⁵⁹ A characteristic of a secure development lifecycle is a focus on security at each phase of the software development lifecycle, from conceptualization to ongoing operation.²⁶⁰ While there are

²⁵⁵ For example, the Multiplexed Information and Computing Service, or Multics, developed in the 1960s, was designed as a secure operating system and was an important influence in shaping future concepts of computer security. *See e.g.*, MIT, “Multics,” <https://web.mit.edu/multics-history/>.

²⁵⁶ Microsoft, “About Microsoft SDL,” *available on* June 11, 2020, <https://web.archive.org/web/20200611020126/https://www.microsoft.com/en-us/securityengineering/sdl/about>.

²⁵⁷ Microsoft, “About Microsoft SDL,” *available on* June 11, 2020, <https://web.archive.org/web/20200611020126/https://www.microsoft.com/en-us/securityengineering/sdl/about>.

²⁵⁸ *See* CISCO, “Trustworthy Solutions,” <https://www.cisco.com/c/en/us/about/trust-center/technology-built-in-security.html#~trustworthysolutionsfeatures~trustworthysolutionsfeatures>; Adobe, “The Adobe Secure Product Lifecycle (SPLC),” <https://www.adobe.com/trust/security/adobe-splc.html>; Romeo, Chris, “Secure Development Lifecycle: The Essential Guide to Safe Software Pipelines,” Security Journey, May 3, 2019, <https://www.securityjourney.com/post/secure-development-lifecycle-the-essential-guide-to-safe-software-pipelines>. *See also*, SAP, *The Secure Software Development Lifecycle at SAP*, 2020, p. 3.

²⁵⁹ *See* OWASP, “OWASP in SDLC,” *available on* October 20, 2020, https://web.archive.org/web/20201020193959/https://owasp.org/www-project-integration-standards/writeups/owasp_in_sdgc/. *See also*, Microsoft, “What Are the Microsoft SDL Practices?,” *available on* January 09, 2019, <https://web.archive.org/web/20190109013652/https://www.microsoft.com/en-us/securityengineering/sdl/practices>.

²⁶⁰ OWASP, “OWASP in SDLC,” *available on* October 20, 2020, https://web.archive.org/web/20201020193959/https://owasp.org/www-project-integration-standards/writeups/owasp_in_sdgc/.

many ways of describing the various phases of software development, a commonly accepted secure development framework includes the following elements:²⁶¹

- a. Requirements Gathering and Analysis, which tries to answer the question (as OWASP says), “What is the system going to do?”;²⁶²
- b. Design, which answers the question, “How is the system going to do it?”. Design activities include performing a threat analysis (known as “threat modeling”) and selecting algorithms, data structures, security measures, and other elements of design that address the threats and risks identified in the threat analysis;²⁶³
- c. Development (or Implementation), in which the actual coding takes place and the selected algorithms are implemented, ensuring that, for example, cryptographic solutions protect data and known vulnerabilities are excluded or mitigated;²⁶⁴

²⁶¹ For simplicity, I am presenting these elements in the order of the classic Waterfall methodology, but the same elements are relevant to other methodologies, including the Agile development methodology.

²⁶² See OWASP, “OWASP in SDLC,” *available on* October 20, 2020, https://web.archive.org/web/20201020193959/https://owasp.org/www-project-integration-standards/writeups/owasp_in_sdgc/. See also, Microsoft, “What Are the Microsoft SDL Practices?,” *available on* January 09, 2019, <https://web.archive.org/web/20190109013652/https://www.microsoft.com/en-us/securityengineering/sdl/practices>.

²⁶³ As I described in my book “Secure Coding – Principles & Practices,” a threat analysis is “the process of examining who is likely to attack a system and how they are likely to attack it.” Undertaking a threat analysis is advisable because, among other things, it “help[s] during the design and implementation of the application by guiding the designer on what defenses to put in place to protect the application.” Graff and Van Wyk (2003) *Secure Coding: Principles and Practices*, p. 144. See also, Microsoft, “What Are the Microsoft SDL Practices?,” *available on* January 09, 2019, <https://web.archive.org/web/20190109013652/https://www.microsoft.com/en-us/securityengineering/sdl/practices>.

²⁶⁴ See OWASP, “OWASP in SDLC,” *available on* October 20, 2020, https://web.archive.org/web/20201020193959/https://owasp.org/www-project-integration-standards/writeups/owasp_in_sdgc/.

- d. Testing (or Verification), in which both static and dynamic security testing are performed,²⁶⁵ as well as “penetration testing,”²⁶⁶ all in an effort to identify and extinguish vulnerabilities in the software before it is deployed; and
- e. Deployment (or Release) and ongoing management, which involves detecting and responding to incidents to address new threats that emerge over time, vulnerabilities that are identified during deployment, as well as changes in the environment that need to be adapted to.²⁶⁷

143. As part of a secure software development methodology, it is widely accepted practice to provide security training to employees. It is also widely accepted practice to separate the development environment and the testing environment from the production environment.^{268,269}

- a. The development environment is where software is made. Often, it will be a sort of sandbox environment designed to allow developers to collaborate in

²⁶⁵ Static tests analyze the source code prior to compilation, and may also analyze the compiled executable version of the software. Dynamic tests, by contrast, perform run-time verification of the fully compiled software to check functionality that is apparent only when all components are integrated and running. *See* Microsoft, “What Are the Microsoft SDL Practices?,” *available on* January 09, 2019, <https://web.archive.org/web/20190109013652/https://www.microsoft.com/en-us/securityengineering/sdl/practices>.

²⁶⁶ Penetration testing is defined as a “method of testing where testers target individual binary components or the application as a whole to determine whether intra or intercomponent vulnerabilities can be exploited to compromise the application, its data, or its environment resources.” (NIST, “Glossary – ‘Penetration Testing’,” *available on* October 19, 2020, https://web.archive.org/web/20201019101437/https://csrc.nist.gov/glossary/term/penetration_testing). *See also* Microsoft, “What Are the Microsoft SDL Practices?,” *available on* January 09, 2019, <https://web.archive.org/web/20190109013652/https://www.microsoft.com/en-us/securityengineering/sdl/practices>.

²⁶⁷ *See* OWASP, “OWASP in SDLC,” *available on* October 20, 2020, https://web.archive.org/web/20201020193959/https://owasp.org/www-project-integration-standards/writeups/owasp_in_sdgc/.

²⁶⁸ In programming, an environment is a collection of internal and external programs, data, and possibly hardware, bundled with different practices and permissions.

²⁶⁹ *See, e.g.*, NIST Cybersecurity Framework, p. 33. (“PR.DS-7: The development and testing environment(s) are separate from the production environment.”).

experimenting, building, and debugging software isolated from other systems. To allow flexibility for innovation, the development environment often does not—indeed, should not—follow the strict security practices of later stages, including production (see below).²⁷⁰

- b. Once a new software component is developed, it is tested in a controlled environment (sometimes a dedicated testing environment, sometimes a fenced-off subdivision of development) that is separate from production but mimics production as closely as possible. The goal of this environment is to identify and resolve any bugs or issues before the new software component goes live.²⁷¹
- c. The production environment (also known as the “operational environment”) is the live environment where the final, tested software is deployed and used by end-users. The production environment is highly secure and expected to be stable, requiring strict change management controls to ensure any updates or changes have been thoroughly tested before integration.²⁷² Performance, security, and

²⁷⁰ See, e.g., OWASP, *Secure Coding Practices: Quick Reference Guide*, November 2010, p. 11. (“Isolate development environments from the production network and provide access only to authorized development and test groups. Development environments are often configured less securely than production environments and attackers may use this difference to discover shared weaknesses or as an avenue for exploitation[.]”). See also, NIST Special Publication 800-53, p. 98. (“Separate baseline configurations allow organizations to apply the configuration management that is most appropriate for each type of configuration. For example, the management of operational configurations typically emphasizes the need for stability, while the management of development or test configurations requires greater flexibility.”).

²⁷¹ See, e.g., NIST Special Publication 800-53, pp. 98, 101. (“Configurations in the test environment mirror configurations in the operational environment to the extent practicable so that the results of the testing are representative of the proposed changes to the operational systems. [...] Analyze changes to the system in a separate test environment before [deployment] in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.”).

²⁷² Humble, Jez and David Farley, *Continuous Delivery*, Pearson Education, 2011, p. 273. (“Production environments should be completely locked down, so that only your deployment pipeline can make changes to it.”).

reliability are critical in production since this is where real users interact with the system, and any issues can have significant business impacts.

2. *The SolarWinds Security Statement made assertions about a secure development lifecycle and security testing*

144. The Security Statement stated that SolarWinds followed a secure software development lifecycle.²⁷³ In particular, the Security Statement asserted the following:²⁷⁴

- a. “We follow a **defined methodology for developing secure software** designed to increase resiliency and security of our products. Security and security testing are implemented **throughout the entire software development methodology**. Quality Assurance is involved at each phase of the lifecycle and security best practices are a mandated aspect of **all development activities**.”^{275,276}

²⁷³ As I explain in footnote 252, the Security Statement appears to have used the terms “secure development lifecycle” and “Software Development Lifecycle” interchangeably.

²⁷⁴ Additionally, the “Trust Center” section on SolarWinds’ public website also stated, under the header “**Secure Development Lifecycle**”: “We follow a defined methodology to develop software designed to increase resiliency and security of our products.” SolarWinds, “SolarWinds Trust Center,” *available on* December 14, 2020, <https://web.archive.org/web/20201214181943/https://www.solarwinds.com/trust-center?promo=blog>.

²⁷⁵ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132. Emphasis added.

²⁷⁶ I understand that SolarWinds staff have testified that the “defined methodology” in the first sentence of this section of the Security Statement refers to “agile” development processes, not SDL. Deposition of Steven Colquitt, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, September 18, 2024 (“Colquitt Deposition”), at 133:17-133:21. (“Q. So as you use the term [in the Security Statement], what does a ‘defined methodology’ mean? A. In this case it’s referring to the Agile processes and the phases that complete that process that we followed within engineering.”). However, based on Mr. Brown’s deposition and contemporaneous correspondence between Mr. Brown and SolarWinds staff, I understand this to refer to the SDL. *See, e.g.*, Brown Deposition, at 130:8-19 (“Q. Is there any difference between secure development lifecycle as it is used here and the term software development lifecycle as it is used in the heading in your mind? A. No. Q. Do you understand that Mr. Colquitt’s initiative in 2018 was titled secure development lifecycle? A. I am. Q. So -- and that initiative was not put into place until sometime after SolarWinds’ security statement was posted to its public facing website, correct? A. Correct.”). *See also* SW-SEC00336293–294 at 293. (Colquitt asks: “I just noticed that we refer to that section as Software Development Lifecycle. I wonder for the sake of consistency if we should have that changed to Secure Development Lifecycle or if we really need to use the word software then Secure Software Development Lifecycle. What do you think?” Brown responds: “We were trying to match the language used in many of the questionnaires we receive. I think of Software Development Lifecycle incorporates [sic] more than Security.”).

b. “Our secure development lifecycle follows **standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments.**”^{277,278}

c. Among the “security best practices” and “standard security practices” that SolarWinds asserted to follow, it stated that “SolarWinds **maintains separate development and production environments.**”²⁷⁹

3. *SolarWinds failed to follow the SDL and security testing procedures as asserted in the Security Statement*

145. Despite the public assertions described above, SolarWinds’ internal communications suggest that senior SolarWinds employees were aware of the fact that SolarWinds did not follow the core steps of the SDL as consistently as described in the Security Statement: “We follow **a defined methodology for developing secure software** designed to increase resiliency and security of our products. Security and security testing are implemented **throughout the entire software development methodology.** Quality Assurance is involved at each phase of the lifecycle and security best practices are a mandated aspect of **all development activities.**”²⁸⁰

146. Failing to perform several core steps of the SDL (such as core security testing before a software was released to the public) not only contradicted the Security Statement; it also

²⁷⁷ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132. Emphasis added.

²⁷⁸ Additionally, while not on the website, the Detailed SolarWinds Security Statement shared with customers upon request also asserted that “[a]ny vulnerabilities that are identified, are fixed.” SW-SEC00292763–781 (Detailed SolarWinds Security Statement dated May 2018) at 777.

²⁷⁹ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 131. Emphasis added.

²⁸⁰ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132. Emphasis added.

violated commonly accepted industry norms and exposed the company and its customers to preventable security risks. As described above, during the Relevant Period, industry bodies and leading industry members (such as OWASP, ISO, the SANS Institute, the CIS, and Microsoft) explicitly recommended following the general steps of a secure development lifecycle.²⁸¹ The industry bodies warned that failure to follow an SDL may expose an organization to several significant risks, including security vulnerabilities in its software and operational disruptions.²⁸²

147. First, without (for example) threat modeling, secure coding, and regular penetration testing—all important steps within the SDL framework—organizations are more likely to develop code that may harbor vulnerabilities that hackers can exploit.²⁸³ The more of these steps an organization skips, the more likely it is to develop code that can be exploited by hackers, leading to data breaches, financial losses, and damage to the company’s reputation—the list of potential catastrophes is long. For instance, untested or poorly secured code might well contain flaws such as inadequate access control mechanisms, allowing attackers to steal sensitive

²⁸¹ See OWASP, “OWASP in SDLC,” *available on* October 20, 2020, https://web.archive.org/web/20201020193959/https://owasp.org/www-project-integration-standards/writeups/owasp_in_sdgc/; ISO/IEC 27001:2013(E), A.14.1-A.14.3; Johnson, Eric, “Secure Software Development Lifecycle Overview,” SANS, April 7, 2015, <https://www.sans.org/blog/secure-software-development-lifecycle-overview/>; CIS, “The 20 CIS Controls & Resources,” *available on* June 19, 2019, <https://web.archive.org/web/20190619213638/https://www.cisecurity.org/controls/cis-controls-list/>; Microsoft, “What Are the Microsoft SDL Practices?,” *available on* January 09, 2019, <https://web.archive.org/web/20190109013652/https://www.microsoft.com/en-us/securityengineering/sdl/practices>.

²⁸² Johnson, Eric, “Secure Software Development Lifecycle Overview,” SANS, April 7, 2015, <https://www.sans.org/blog/secure-software-development-lifecycle-overview/> (“Failing to include software security in the development lifecycle has many consequences: [r]eleasing critical vulnerabilities to production, [p]utting customer data at risk, [c]ostly follow-up releases to secure the application, [d]evelopment teams believing security is someone else’s job, [a]nd the list goes on?”).

²⁸³ See, e.g., Thurmond, Tori, “8 Best Secure Coding Practices,” KirkpatrickPrice, *available on* September 27, 2020, <https://web.archive.org/web/20200927124111/https://kirkpatrickprice.com/blog/secure-coding-best-practices/> (“[S]oftware developers are expected to uphold secure coding standards to ensure they aren’t leaving any vulnerabilities open for hackers to exploit.”); OWASP, “Threat Modeling: OWASP Cheat Sheet Series,” *available on* July 16, 2019, https://web.archive.org/web/20190716105548/https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html (“In general, the threat modeling will help designers, architects and assessors discover logical attacks.”).

customer data or disrupt services.²⁸⁴ Such security flaws can also make the company an easier target for cybercriminals and could lead to significant compliance violations, especially in industries governed by strict data protection regulations like GDPR.²⁸⁵

148. Second, operational disruptions are also more likely to occur if an organization fails to sufficiently test software for security issues during the development phase. Vulnerabilities that are not caught early in the design or development process often require urgent fixes after a product is deployed, which can lead to time- and cost-intensive remediation, including service outages and high incident response costs.²⁸⁶ Fixing vulnerabilities post-deployment is typically more expensive and time-consuming than addressing them during development, potentially causing delays and financial losses.²⁸⁷

149. As I find below, senior SolarWinds employees were aware that the company did not consistently follow best practices for secure software development, and that the company and

²⁸⁴ Graff and Van Wyk (2003) *Secure Coding: Principles and Practices*, p. 142 (“Test environments and practices are vital parts of a sound configuration management process. The reasons for this are numerous, starting with the fact that it’s a good practice to verify configurations (and changes) in an environment that can’t possibly adversely impact the business processes supported by the production version of the application. Although this sounds like common sense, we’ve often been surprised to find production applications that go through no such testing.”). *See also* Graff and Van Wyk (2003) *Secure Coding: Principles and Practices*, p. 158. (“[W]e need to squeeze out as many vulnerabilities as we can, retest often, and plan carefully to mitigate the risks associated with the latent bugs we miss.”).

²⁸⁵ *See* PA Consulting, *GDPR - How Is Industry Addressing the Legislation*, January 25, 2017, p. 22.

²⁸⁶ *See, e.g.*, Graff and Van Wyk (2003) *Secure Coding: Principles and Practices*, p. 18. (“If [a] software had been tested and deployed properly, someone would have noticed [a security] problem before it affected thousands of Internet sites and cost millions of dollars in lost time, data, and opportunity.”).

²⁸⁷ *See, e.g.*, NIST, *The Economic Impacts of Inadequate Infrastructure for Software Testing*, May 2002, p. 5-3. (“The relative cost (also referred to as cost factors) of repairing defects found at different stages of software development increases the longer it takes to find a bug.”). *See also* CISA, *Development of Secure Software with Security by Design*, July 2014, p.1. (“The earlier such a security process detects vulnerabilities during the development, the lower the costs for a remedy. Implementing security measures after the fact is significantly more expensive and usually offers less protection than security that was integrated into the system development process or into the product selection process from the very beginning.”).

its customers were therefore potentially vulnerable to the security and operational risks such as those described above.

a. Internal documents contradicted the assertion that SolarWinds maintains separate development and production environments

150. In contradiction with the public statement that “SolarWinds maintains separate development and production environments,”²⁸⁸ the documents that I have reviewed (and which I describe below) indicate that this was not consistently the case during the Relevant Period.²⁸⁹ To explain why this inconsistency between SolarWinds’ internal practices and its Security Statement is particularly serious from a cybersecurity perspective, I show below that SolarWinds’ failure to separate the development environment from the production environment was a substantial violation of commonly accepted industry norms. The internal documents that I have reviewed indicate that senior SolarWinds employees were aware of this security violation and its potentially grave consequences.

151. Industry bodies (including NIST and the ISO) agree that, without separating the development and production environments, organizations increase the “risk of unauthorized access or changes to the operational environment.”²⁹⁰ Conversely, without separating the production environment from development, companies increase the risk of an attacker being able access and modify the company’s products—which, as Mr. Brown testified, are considered

²⁸⁸ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 131.

²⁸⁹ SW-SEC00168780 at tab ‘7.13.2020 Review’, cell C9 (“Developers have write access to production Backup data”); SW-SEC00254254–266 at 265 (“The developers are developing in Production as the staging/dev environments are not suitable.”).

²⁹⁰ ISO/IEC 27001:2013(E), A.12.1.4. (“Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.”). *See also* NIST Cybersecurity Framework at p. 33. (“PR.DS-7: The development and testing environment(s) are separate from the production environment.”).

SolarWinds’ “critical assets.”²⁹¹ In other words, an attacker who compromised a company’s outward-facing website might move laterally into the development network, using a connection between production and development, and potentially modify the product source code.

152. This is a well-known issue that I wrote about more than 20 years ago. In my book published in 2003, I explained why a lack of proper separation between production and development environments can amplify a system’s exposure to security risks.²⁹² For instance, in 2001, a computer worm²⁹³ named “Code Red” infected computers worldwide. Though the Code Red worm had been discovered prior to the incident, and many companies had applied patches to protect their systems, vulnerabilities remained due to poor environment separation. In one case, a company had successfully patched its production systems to safeguard against the worm. However, because some computers in the development and production environments had direct communication channels with one another, the worm was able to re-infect the production systems after bypassing their firewalls via breaching the development environment.²⁹⁴ The incident showed that failure to isolate the development and production environments can expose critical systems to security threats, *despite taking other protective measures*.²⁹⁵

153. Furthermore, developing software in the production environment can also lead to operational risks such as deploying unstable code (due to introducing bugs or errors), accidental

²⁹¹ Brown Investigative Testimony, Vol. I, at 53:13-25.

²⁹² See Graff and Van Wyk (2003) Secure Coding: Principles and Practices, pp. 129-155.

²⁹³ A computer worm is a type of malicious software that replicates itself and spreads across computers, typically through a network. NIST, “Glossary – ‘Worm,’” *available on* August 13, 2020, <https://web.archive.org/web/20200813182531/https://csrc.nist.gov/glossary/term/worm>.

²⁹⁴ Graff and Van Wyk (2003) Secure Coding: Principles and Practices, pp. 152-153.

²⁹⁵ The lack of separation between production and development environments continues to be exploited by attackers. For a description of recent incidents *see e.g.*, Evans, Woody, “3 Ways to Mitigate the Growing Risk of Non-Production Environment Breaches,” Delphix, March 28, 2023, <https://www.delphix.com/blog/3-ways-to-mitigate-the-growing-risk-of-non-production-environment-breaches>.

modifications, regulatory non-compliance, and increased downtime risks.²⁹⁶ Moreover, shared environments typically make diagnosing issues and rolling back changes more difficult, complicating overall system management. Senior SolarWinds employees were aware of the risk posed by not separating their production and development environments, as exemplified by Mr. Quitugua’s testimony on the importance “that any changes within the development and staging environments don’t affect production systems that could potentially bring down and make them unavailable for [...] the services that [SolarWinds] provide[s].”²⁹⁷ Of course, as I described elsewhere, there are several other important risks that result from the lack of separation between these environments.

154. Despite the above well-known security and operational risks resulting from a failure to separate the production and development environments, internal documents suggest that SolarWinds employees were aware that the company did not consistently implement this industry norm. In an email chain from November 2019, various SolarWinds employees (including Mr. Brown, Ms. Johnson, and Mr. Quitugua) discussed the failure to separate the development environment from the production environment.²⁹⁸

155. Senior SolarWinds employees were clearly aware of the gravity of the issue of the lack of separation between the development and production environments. They described this incident as “a significant security [...] violation” that “needs to stop immediately” and that

²⁹⁶ See, e.g., Humble, Jez and David Farley, *Continuous Delivery*, Pearson Education, 2011, p. 273. (“Most downtime in production environments is caused by uncontrolled changes. Production environments should be completely locked down, so that only your deployment pipeline can make changes to it. That includes everything from the configuration of the environment to the applications deployed on it and their data.”).

²⁹⁷ Quitugua Investigative Testimony, Vol. I, at 134:9-17. (“Q From a security standpoint, is it important for the development staging, testing, QA, and production environment to be separated? A Yes. Q Why? A So that any changes within the development and staging environments don’t affect production systems that could potentially bring down and make them unavailable for -- for the services that they provide.”).

²⁹⁸ SW-SEC00254254–266.

“under no circumstances” should have happened,²⁹⁹ it was “poor security practice,”³⁰⁰ “clearly bad,” and an “ISO violation” that “need[ed] to be filed as a non-conformity and reported.”³⁰¹

They also stated this violation failed the cybersecurity principle of separation of duties (which I described in **Section III.A**).³⁰² I agree with these SolarWinds employees’ opinion that this issue was a major security violation that did not conform to commonly accepted industry practices and that violated the basic tenets of cybersecurity.

156. Importantly, based on SolarWinds employees’ discussions, this issue was not a one-off incident, but as an ongoing, recurring pattern. For example, when questioned about this practice by his superiors, a Senior Product Manager responded that “it’s not something new, we were developing billing using production services since the beginning.”³⁰³ When discussing this incident with his colleagues, Mr. Quitugua also stated that SolarWinds “ha[s] experienced security incidents because of errors made when accessing production data and have also had to

²⁹⁹ SW-SEC00254254–266 at 265. (From Chris Day, VP of Global DevOps and Technology Operations: “Hello – highlighted item [The developers are developing in Production] needs to stop immediately. Under no circumstances is development to be done in production. If that impacts deliverables please let August know. That is a significant security and Sox violation. As part of our ISO it also need to be filed as a non-conformity and reported.”).

³⁰⁰ SW-SEC00254254–266 at 260. (From Eric Quitugua, Senior Manager, Information Security: “[...] the risk being brought up by the MSP DevOps team is valid. I can’t stress enough that any request made to make production data available to test and development environments need to be vetted through the security team. Acceptance of this type of risk cannot be made by your teams. We have experienced security incidents because of errors made when accessing production data and have also had to document compliance violations because of this poor security practice. Let’s continue to work together to make sure this doesn’t happen again.”).

³⁰¹ SW-SEC00254254–266 at 257. (From Chris Day, VP of Global DevOps and Technology Operations: “This is a separation of duties and a control issue that needs to be decided between Tim O, Rani, and Tim Brown. It is clearly bad - violation of SOX controls and an ISO violation that we will need to register as there is no separate of duties and developers have full access to a billing environment (which we need to file regardless as it already exists).”); SW-SEC00254254–266 at 265. (From Chris Day: “Hello – highlighted item [The developers are developing in Production] needs to stop immediately. Under no circumstances is development to be done in production. If that impacts deliverables please let August know. That is a significant security and Sox violation. As part of our ISO it also need to be filed as a non-conformity and reported.”).

³⁰² SW-SEC00254254–266 at 257. (From Chris Day, VP of Global DevOps and Technology Operations: “[...] This is a separation of duties and a control issue[.]”).

³⁰³ SW-SEC00254254–266 at 264-265. (From Andrey Rodushkin, Senior Product Manager: “As far as I know it’s not something new, we were developing billing using production services since the beginning as only production has data to test billing.”).

document compliance violations because of this poor security practice,” indicating that several similar issues have occurred in the past.³⁰⁴

157. The fact that such a fundamental issue, which violated industry norms and could cause catastrophic issues could persist for a prolonged period of time, with the knowledge of senior employees, is in my opinion indicative of systemic issues at SolarWinds.

158. Additionally, SolarWinds employees described this issue being so systemic that it would take considerable effort to resolve. For example, when asked by Chris Day to “stop immediately,” a Senior Product Manager told him that “if you want to stop it, okay, but it affects a lot of stuff: billing platform development/support and new O365 [Microsoft 365] billing as well.”³⁰⁵ Sergey Smolsky (Director of Engineering) agreed, warning that addressing this issue “will require efforts from Backup Engineering/DevOps to obfuscate production data and have enough test data to avoid going to production. We need to plan these activities and prepare this environment.”³⁰⁶ Other employees stated that while they “would love to” separate the development and the production environments, SolarWinds’ current systems were not set up in a way that would make this feasible.³⁰⁷ They also stated that “[w]e’ve been trying to move them to

³⁰⁴ SW-SEC00254254–266 at 260.

³⁰⁵ SW-SEC00254254–266 at 264-265. (From Andrey Rodushkin, Senior Product Manager: “As far as I know it’s not something new, we were developing billing using production services since the beginning as only production has data to test billing. And if you want to stop it, okay, but it affects a lot of stuff: billing platform development/support and new O365 billing as well.”).

³⁰⁶ SW-SEC00254254–266 at 264. (From Sergey Smolsky, Director of Engineering: “The problem that Andrey has brought up (incomplete billing data in test environment) will require efforts from Backup Engineering/DevOps to obfuscate production data and have enough test data to avoid going to production. We need to plan these activities and prepare this environment.”).

³⁰⁷ SW-SEC00254254–266 at 258. (From Sean O’Shea: “When thinking about the separation of developers from production systems what is the justification for them just not having this access is dev/staging only? Good question, I would love to develop only on staging, but our billing system is complicated and our staging doesn’t reflect production customer tree and also staging doesn’t have all billing cases which we have in production. We’ve been trying to move them to staging for a while, but it’s hard to resolve [.]”).

staging for a while, but it's hard to resolve items above ... [sic]".³⁰⁸ The fact that employees were not able to conform to the best practice described within the Security Statement despite their best efforts is, again, indicative of a systemic issue, rather than a one-off mistake.

159. Even after being alerted that SolarWinds had this major security violation (which directly violated the assertion in the public Security Statement), SolarWinds employees appear not to have prioritized addressing this security issue. In fact, the violation appears to have gone unaddressed for at least eight months after Mr. Brown was alerted of the problem on November 14, 2019.³⁰⁹ Although a Risk Acceptance Form (RAF) indicates that, in November 2019, Mr. Brown reviewed and accepted this risk for it to be addressed by January 31, 2020,³¹⁰ this risk was still unaddressed by the June 8, 2020 and July 13, 2020 RAF meetings.³¹¹ I have not found a document indicating when this issue was ultimately addressed.

160. In the face of this severe vulnerability, which represented a contradiction of the Security Statement, several SolarWinds employees appear to have explicitly advocated for delaying addressing this major security issue in order to avoid a negative impact on SolarWinds' business. For example:

- a. Tim Brown: "As with a number of the issues we deal with it looks like this is going to take some time to appropriately design and resolve. We have built our RAF Risk Acceptance Form model for these cases. We should not disrupt

³⁰⁸ SW-SEC00254254–266 at 258.

³⁰⁹ SW-SEC00254254–266 at 262-263.

³¹⁰ SW-SEC00168780, at tab '7.13.2020 Review,' cell F9 (under column "Risk Acceptance Expiration (date by which risk will be remediated)" and value: "1/31/2020") and cell M9 (under column "Compensating Control" and value: "11/18/19: Risk review by and accepted by Tim Brown.").

³¹¹ SW-SEC00168778–779 at 778. ("Recap of 6/8 Risk Review meeting:"). The risk acceptance deadline of item #9 expired on January 31, 2020 ("#9: BizApps DB, RA expires 1/31/2020 - Sent Rick note asking for status update").

business, we should file a RAF accept risk for a period of time so that we can develop the correct approach.”³¹²

- b. Alex Quilter: “[...] potential financial impact to MSP via Backup. I want to ask everyone to work towards finding us a solution we can put in place to keep us moving forward. We have a tight roadmap/release scheduled for December, and can’t spin our wheels on this one too long.”³¹³
- c. Andrey Rodushkin: “While you thinking what options we have, please keep in mind that current users are used for Backup billing, and if we remove access then we lose all Backup money ... [sic]”³¹⁴

161. In line with the priorities expressed above by SolarWinds employees, this email chain and the corresponding RAF forms indicate that SolarWinds decided to continue operations without segregating the production and development environments.³¹⁵ Even though the senior SolarWinds employees on the email chain agreed that this was a major security violation, as I show below, both the “Short-Term Solution” and the “Long-term Solution” failed to even contemplate separating the production data from the development environment (and thus complying with the Security Statement). Specifically:

³¹² SW-SEC00254254–266 at 256.

³¹³ SW-SEC00254254–266 at 259.

³¹⁴ SW-SEC00254254–266 at 259.

³¹⁵ SolarWinds addressed the shared login issue discussed above, but not the issue that developers had access to the production data. SW-SEC00254254–266 at 255.

- a. The short-term solution focused only on granting the developers with “Superuser” access to the production data so “we could move forward with our [...] project.”³¹⁶
- b. The long-term solution, which was planned to be undertaken by “the first 2 weeks of January” (*i.e.*, six-to-eight weeks after the issue was identified), still did not separate production from development—it simply planned to revoke the developers’ “write” access, while keeping their “read” access to production.³¹⁷

This interim fix, which SolarWinds described as a “Long-term Solution,” still would not have addressed the problem that I pointed out above, that a bridge between the production and development environments afford a potential path for lateral movement by potential attackers. In other words, even the “Long-term Solution” would not have complied with the Security Statement. Additionally, as described above, according to the RAF, the issue was still not addressed as of July 13, 2020,³¹⁸ therefore, even the “first 2 weeks of January” deadline was missed by at least six months.
- c. It was only what SolarWinds described as the “Longer-term solution,” planned to be undertaken at an undisclosed time in the future, that planned to separate the production environment from the development environment (interposing a “test

³¹⁶ SW-SEC00254254–266 at 255. (“Short-Term Solution: BizApps would be granted Superuser access to the new API which would unblock us and we could move forward with our Backup 0365 billing project.”).

³¹⁷ SW-SEC00254254–266 at 255. (“Long-term Solution: Create Read-only role that BizApps would use to access production data for Backup billing and for Backup O365 billing. This work would take approximately 2 weeks but as the Backup team has some commitments they are wrapping up, a likely go-live with this role would be in the first 2 weeks of January.”).

³¹⁸ SW-SEC00168780, at tab ‘7.13.2020 Review,’ cell O9 (under column “Risk Status” and value: “Remediation In Progress”).

environment”).³¹⁹ Therefore, it was only this “Longer-term solution” that even contemplated compliance with the Security Statement.

162. Overall, I have seen no evidence indicating that SolarWinds had a mechanism to ensure the accuracy of the public assertion in their Security Statement that “SolarWinds maintains separate development and production environments.”^{320,321} In this specific case, not only did they leave this highly risky configuration and practices in place for a prolonged period of time, but the Security Statement remained static despite senior SolarWinds employees knowing that what it said about the separation of development and production environment was actively being violated, and that the potential implications of this violation exposed the company and its customers to substantial risks.

b. Internal documents and testimony contradicted the assertion that security best practices were a mandated aspect of all development activities

163. In contradiction with the public statement that security testing is implemented “throughout the **entire** software development methodology” and that “security best practices are a mandated aspect of **all** development activities,”³²² Mr. Brown testified that SolarWinds did not consistently apply the SDL when developing internally built solutions. According to Mr. Brown,

³¹⁹ SW-SEC00254254–266 at 255. (“Longer-term solution for after we get migrated to the Billing Platform and work on subsequent features and projects: After we get our billing migrated to the Billing Platform, we would like to have a TEST environment where we could test new features against before moving those features to production. This new test Backup environment would require several servers to be created to host it.”).

³²⁰ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 131.

³²¹ I understand that despite acknowledging the importance of separating the development and production environments, Mr. Brown continues to assert that “we did maintain separate development testing and production environments within SolarWinds.” Brown Deposition, at 148:23-149:21. (“Q. [...] there’s a statement, ‘The development and testing environment(s) are separated from the production environment.’ [...] Do you see that, sir? [...] A. Yeah, development and testing environments are separate from the production environment. [...] we did maintain separate development testing and production environments within SolarWinds.”).

³²² SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132. Emphasis added.

these internally built solutions, known as business applications or “BizApps,”³²³ “do things like support our billing, that help us manage our customers, that help us generate lists of customers to send emails to.”³²⁴ In fact, Mr. Brown testified that, as of June 2020, one of the BizApps known as the Orion Improvement Program (“OIP”) “was not under SDL.”³²⁵ He also testified that BizApps “have a different set of testing, different set of requirements” than “products that customers get,” which “are under SDL.”³²⁶

164. However, the Security Statement failed to specify the fact (which I show below is important) that the SDL applied only to products sold to customers—but *not* to internal software that SolarWinds used to support and manage these same products. Neither did the Security

³²³ It appears that the term “BizApps” referred both to the business applications and to the team that created these applications. *See* Brown Deposition at 270:24-271:9. (“Q. [...] What is BizApps in your understanding? A. So BizApps is a group that reported to Rani Johnson. BizApps were produced internal products or internal solutions. So Salesforce is our way that we manage customers, a way that we contact customers. We built applications in Salesforce, for example. BizApps produces those applications. Q. So were the BizApps sold to customers or were they solely used within SolarWinds? A. Solely used within SolarWinds.”).

³²⁴ Brown Investigative Testimony, Vol. II at 394:16-395:4. (“A And some of the other components that are built through our Bizapps team [...] [were] not going through that SDL process. [...] Products are under SDL, products that we ship are under SDL. Products that customers get are under SDL. We have a number of internally built solutions, we’ll call them solution, that do things like support our billing, that help us manage our customers, that help us generate lists of customers to send emails to. So these are called Bizapps, business applications.”).

³²⁵ Brown Investigative Testimony, Vol. II at 394:15-395:23. (“A [...] We’ve been working to get all of the products that are built by Bizapps under SDL [...] [b]ut at this point in time [OIP] was not under SDL. Therefore what we did was do evaluation on it and bring it under SDL.”).

³²⁶ Brown Investigative Testimony, Vol. II at 394:23-395:21. (“Products are under SDL, products that we ship are under SDL. Products that customers get are under SDL. [...] [BizApps] have a different set of testing, different set of requirements.”).

Statement explain that these internal solutions—which, again, were related to the products—had different testing and security requirements.

165. In fact, the Security Statement stated the following:

“We follow a defined methodology for developing secure software that is designed to increase the resiliency and trustworthiness of our products.”

166. Despite Mr. Brown’s interpretation,³²⁷ in my opinion, this sentence does not indicate that the SDL was applied to SolarWinds’ for-sale products alone, and not to internal software that SolarWinds used to support and manage these same products. In fact, if they had not applied a secure software development process “throughout the **entire** software development methodology” and to “**all** development activities”—which is precisely what the Security Statement asserted the company did—that would tend to diminish the “resiliency and trustworthiness”³²⁸ of its products, if the insecurity of their internal software allowed attackers to corrupt or diminish the integrity of its products’ software.

167. My interpretation (that the Security Statement did not make it clear that SolarWinds’ internal software supporting its products were not under SDL) is also supported by the Security Statement’s assertion that SolarWinds’ assets, including “customer and end-user

³²⁷ Brown Deposition at 123:13-24, 271:7-14. (“Q. The first sentence states, ‘We follow a defined methodology for developing secure software that is designed to increase the resiliency and trustworthiness of our products.’ To your understanding, was that statement accurate when the security statement was published on the SolarWinds’ website? A. Yes, we had a -- a defined methodology to build products. We had defined groups for, uh, the major functions of product development, uh, and that our software is -- is designed, uh, designed for to be to increase resiliency and trustworthy of our product. [...] Q. So were the BizApps sold to customers or were they solely used within SolarWinds? A. Solely used within SolarWinds. Q. Were those developed pursuant -- pursuant to SolarWinds’ secure development lifecycle? A. Uh, they -- they were not products. So as the statement says, it’s for products. So products go through this cycle.”).

³²⁸ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132. Emphasis added.

assets *as well as corporate assets*” were “managed under our security policies and procedures.”³²⁹

168. As I describe below, my interpretation (that the Security Statement did not make it clear that SolarWinds’ internal software supporting its products were not under SDL) is also consistent with the fact that, in June 2020, several SolarWinds employees recommended that “[i]f SDL is not enforced for OIP, we should do it ASAP.”³³⁰

169. I also note that, in his deposition, Mr. Brown stated that one reason why BizApps were not built under SDL was that they were often extensions to third-party (*e.g.*, Salesforce or NetSuite) applications, and that SolarWinds was not able to do vulnerability scans against third-party applications.^{331,332} However, as Mr. Brown testified during his investigative testimony, “OIP was built internally” and not with Salesforce.³³³ It therefore does not follow that SolarWinds could not have run vulnerability scans on OIP. Indeed, as I describe below, SolarWinds ultimately decided to bring OIP under SDL.³³⁴ During his investigative testimony, Mr. Brown also stated that SolarWinds has “been working to get all of the products that are built

³²⁹ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 129. Emphasis added.

³³⁰ SW-SEC00000673–678 at 677-678. (“If SDL is not enforced for OIP, we should do it ASAP and consider additional actions to make sure that OIP is very well protected.”) *See also* “I don’t believe we cover OIP today with the SDL, but we should.”.

³³¹ Brown Deposition at 272:25-273:1. (“[B]ecause Salesforce is a hosted application run by a third party. You can’t do a scan against them.”).

³³² In my opinion, Mr. Brown’s assertion is incorrect about his observation that “you can’t do a scan against” applications run by a third party. Additionally, there are many ways (other than vulnerability scans) to evaluate the vulnerabilities of a third-party software.

³³³ Brown Investigative Testimony, Vol. II, at 395:4-20. (“One of those business applications is OIP. That business application was built internally [...]. [...] We build custom applications with salesforce.com. This one isn’t [...].”).

³³⁴ *See, e.g.*, SW-SEC00459171–305 at 238-239, 248. (“*Calvert, Brian (7/17/2020)*: [...] OIP Server doesn’t have an SDL yet[...] [...] SDL is considered mid-term (Q3) but that’s not officially scheduled yet[...] [...] *Calvert, Brian (8/19/2020)*: Wanted to circle back with you helping BizApps and WebDev follow SDL[.]”). *See also*, Brown Investigative Testimony, Vol. II, at 394:5-23. (“A [...] We’ve been working to get all of the products that are built by Bizapps under SDL [...] [b]ut at this point in time [OIP] was not under SDL. Therefore what we did was do evaluation on it and bring it under SDL.”).

by Bizapps [sic] under SDL;” with respect to OIP, he specifically added that SolarWinds decided to “bring it under SDL.”³³⁵ In other words, Mr. Brown’s explanation that some BizApps were not under SDL because SolarWinds was not able to do a scan against them did not apply to OIP. Indeed, Mr. Brown testified that bringing OIP under SDL involved “get[ting] Checkmarx going, get[ting] WhiteSource going” which were the code scanning tools SolarWinds used in its SDL processes.³³⁶

170. Additionally, while it is true that OIP was not a stand-alone product that customers outright purchased from SolarWinds, OIP was nevertheless used by customers. OIP was a component made available for customer installations of Orion,³³⁷ which was a product that Mr. Brown explicitly described as one of SolarWinds’ “critical assets.”³³⁸ According to Mr. Brown and the SolarWinds website, OIP was developed internally to collect “evaluation, performance, and usage data from SolarWinds users to determine ways [SolarWinds] products

³³⁵ Brown Investigative Testimony, Vol. II, at 395:15-23. (“A [...] We’ve been working to get all of the products that are built by Bizapps under SDL [...] [b]ut at this point in time [OIP] was not under SDL. Therefore what we did was do evaluation on it and bring it under SDL.”).

³³⁶ Brown Investigative Testimony, Vol. II, at 399:7-17. (“Q Okay. All right, so Mr. Vrael sends this email. [...] ‘I don’t believe we cover OIP today with the SDL but we should.’ A Yep. Q And [...] do you understand why he says ‘we should?’ A Yep. [...] To get a final security review going, get Checkmarx going, get WhiteSource going, conduct final security review of all of the rest [...].”). *See also*, Brown Deposition, at 198:10-20 (“Q. I believe you testified Mr. Colquitt’s [SDL] initiative started around January of 2018. A. Correct. Q. So why are you still at a 2 in August [20]19 if that initiative had started in January of [20]18? A. Because we’ve implemented new technology under that program. So we’ve, uh, acquired a product called Checkmarx that we expect to be run on every program, every product. We’ve acquired a product called Whitesource that does OpenSource scanning. So we expect that to be deployed everywhere.”) at 240:5-7 (“A. [C]ode analysis could be Checkmarx, Whitesource. It could -- could be implementing tools across the platform.”).

³³⁷ SW-SEC00000673–678 at 676. (“Oh, yikes, I often forget that on-prem Orion already has a SaaS endpoint open to the public Internet - OIP. Sounds pretty important, I didn’t realize it’s possible an attacker could use it to take over all customer installations.”).

³³⁸ Brown Investigative Testimony, Vol. I, at 53:13-24. (“[Mr. Brown:] But critical assets are things that -- things such as our products, things such as our SAS [sic] services, things like our financial system, things that could cause an event, that could cause an event that would be, you know, harming to the company. Those are what are considered critical. They would now be either considered mission or business critical assets. [...] Q I heard you say it would include products, so that would mean it includes Orion, for instance? A Yep, it includes Orion.”).

may be improved,” and to “help[] customers with their deployment” of SolarWinds products.³³⁹ Customers with an Orion product license had the option to opt out of OIP, but by default they participated in sharing their Orion-related data including user identification, user device, and Orion and SolarWinds product-specific usage data.³⁴⁰ Therefore, OIP operated as *a direct connection* between the Orion product on customers’ computers and SolarWinds’ OIP server.^{341,342}

171. As a result of this relationship between OIP and Orion, a June 2020 email exchange among SolarWinds employees openly discussed that vulnerabilities in OIP (including the OIP server)—which was *not* under SDL³⁴³—had the potential to have a direct detrimental effect on SolarWinds’ Orion product—which *was*, in theory, under SDL.³⁴⁴ Again, the Security

³³⁹ Brown Investigative Testimony, Vol. II, at 394:20-395:12. (“[OIP] was built internally for the specific purpose of collecting information and helping customers with their deployment.”). *See also* SolarWinds, “Orion Improvement Program,” first published on October 15, 2018, last published on January 7, 2022, https://solarwindscore.my.site.com/SuccessCenter/s/article/Orion-Improvement-Program?language=en_US.

³⁴⁰ SolarWinds, “Orion Improvement Program,” first published on October 15, 2018, last published on January 7, 2022, https://solarwindscore.my.site.com/SuccessCenter/s/article/Orion-Improvement-Program?language=en_US. (“You automatically participate in the Orion Improvement Program during an evaluation of SolarWinds software, and you can opt out of participating in the Orion Improvement Program upon the transition to a production license. Upon opting out of the Orion Improvement Program, SolarWinds will not collect any of the data related to the Program from you.”; “the following is an example of data collected [...] when you participate in the Orion Improvement Program: •The SWID (SolarWinds ID) associated with any SolarWinds commercial licenses installed. •The email address provided to the installer during installation. [...] •Operating system version. •CPU description and count. •Physical memory installed and percent used. [...] •Dates when you logged in to the Orion website. •Licensing information of other SolarWinds Orion products locally installed. [...] •Data about devices and applications monitored: ◦Vendor[,] ◦Model[,] ◦OS/Firmware version[,] ◦Count[,] ◦Abstract configuration information, such as number of websites hosted[,] •Data about the SolarWinds product: ◦Feature usage statistics[,] ◦Performance statistics[,] ◦Hardware and OS platform description”).

³⁴¹ I understand that by not opting out of the program, customers had the OIP software installed on their computers. Later, customers could decide to either disable or uninstall OIP. *See* SW-SEC00578414–476 at 414. (“[I]f they have problem with SWIP/OIP it can be turned off or better completely uninstalled”).

³⁴² I note that this is inconsistent with Mr. Brown’s testimony that BizApps were “Solely used within SolarWinds.” Brown Deposition at 271:7-9.

³⁴³ Brown Investigative Testimony, Vol. II at 394:15-395:23. (“A But at this point in time [OIP] was not under SDL.”)

³⁴⁴ Brown Investigative Testimony, Vol. II at 394:23-25. (“Products are under SDL, products that we ship are under SDL. Products that customers get are under SDL.”).

Statement’s broad assertion that “security testing [was] implemented throughout the entire software development methodology” and that “security best practices are a mandated aspect of all development activities”³⁴⁵ failed to convey the fact that OIP, a default component of Orion, had less stringent security testing requirements.

172. This June 2020 email exchange indicates that SolarWinds employees considered several vulnerabilities in OIP to pose a significant threat to Orion. For example, one employee warned that “[i]f the OIP server is compromised, consequences can be disastrous—ranging from [...] collection of customer credentials to attacks like taking over all customer installations.”³⁴⁶ Another employee added: “Oh, yikes, I often forget that on-prem[ises] Orion already has a SaaS [software as a service] endpoint open to the public Internet – OIP. Sounds pretty important, I didn’t realize it’s possible an attacker could use it to take over all customer installations.”³⁴⁷

173. SolarWinds employees then discussed several specific OIP vulnerabilities and the detrimental effects they could have on Orion and on SolarWinds customers. For example, employees discussed that because there was “no restriction” on the commands that could be run on OIP, an attacker could create a “reverse shell.”³⁴⁸ A reverse shell is a severe security threat

³⁴⁵ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132. Emphasis added.

³⁴⁶ SW-SEC00000673–678 (Email from Tomas Vrabel on June 23, 2020) at 678. (“OIP API is not authenticated so it can accept content for any user, API is exposed externally so everybody can access it. If the OIP server is compromised, consequences can be disastrous — ranging from simple XXE attacks or collection of customer credentials to attacks like taking over all customer installations.”).

³⁴⁷ SW-SEC00000673–678 (Email from Chris Erway on June 24, 2020) at 676.

³⁴⁸ SW-SEC00000673–678 at 674-675. (“Yeah, and even more dangerous attack vector: OIP XMLs contain SQL queries but I’m not sure whether it can contain also INSERT/UPDATE commands. [...] In case attacker can run arbitrary command in customer installation, nothing is easier than configure alert that always triggers with actions that will create some malicious vbs file (like reverse shell) and immediately execute it in other alert action.” “[T]here is no restriction on the SQL commands that can be run.”).

that enables an attacker to remotely compromise a victim's entire machine.³⁴⁹ Once a hacker takes over a customer's computer in this way, the attacker may be able to use this compromised computer as a platform from which to attack the customer's network.

174. Additionally, employees discussed the possibility that, if hackers exploited certain vulnerabilities in OIP, "they can definitely collect the data from the orion [sic] system."³⁵⁰ In other words, through these attacks, hackers could hijack the data collection process which customers expect SolarWinds to securely control as part of the Orion Improvement Program. As one employee noted, "if the OIP server is compromised," hackers could send query files which would return the customers' Orion data to the server to which the hackers had access.³⁵¹ Another employee raised the "possible attack vector" that hackers could also change the routing rules on a compromised OIP system installed on a customer's computer, which would redirect the customer's data to go to the hacker's server instead of to SolarWinds' server.³⁵²

175. Similarly, a July 31, 2020 internal security report stated that because OIP did not verify whether certificates came from "solarwinds.com" when following redirects and loading

³⁴⁹ See, e.g., SANS Institute, *Inside-Out Vulnerabilities, Reverse Shells*, May 25, 2006, p. 5 ("Reverse shells create a covert channel that allows an attacker to target specific systems, users, and data. Once installed, reverse shells can allow an attacker to scan your network internally, install network sniffers, collect usernames/passwords, and send your data outside your network."); p. 9 ("Reverse shell programs target systems located inside an internal protected network and force them to connect to a system outside of that protected network. This allows the system located on the external network to communicate with the internal system without having ingress access through the firewall into the protected network.").

³⁵⁰ SW-SEC00000673-678 at 675. (Chandrasekhara Yerasi: "Through this attack, they can definitely collect the data from the orion system.").

³⁵¹ SW-SEC00000673-678 at 675. (Chandrasekhara Yerasi: "The one attack path that we need to analyze and harden for the customer installations if the OIP server is compromised is the following - OIP client on the customer orion install downloads [sic] updated OIP XML query files for installed modules (with basically SWQL/SQL queries that can be executed on the local system). The format of the files downloaded is 'Module-Name.xml'. Through this attack, they can definitely collect the data from the orion system.").

³⁵² SW-SEC00024906-914 at 908-909. ("[Tim and Chandra] said that Orion will follow HTTP redirects served by OIP or someone impersonating or intercepting api.solarwinds.com, so if someone was able to change URL routing rules to send OIP traffic to myhackerserver.com, that is a possible attack vector.").

content, if—as a result of an attack—the OIP client was “redirected from api.solarwinds.com to a site controlled by an attacker, it would load and use malicious content.”³⁵³

176. In the June 2020 email exchange, SolarWinds employees recommended that “[i]f SDL is not enforced for OIP, we should do it ASAP and consider additional actions to make sure that OIP is very well protected.”³⁵⁴

177. In fact, one engineer noted that he found a vulnerability in OIP that likely would not have been present if OIP had been developed under SDL. He explained his discovery that the OIP server was using a well-known and publicly available vulnerable library.³⁵⁵ Vulnerable libraries are software components that incorporate publicly known cybersecurity vulnerabilities, which hackers can easily exploit.³⁵⁶ This discovery made him “strong[ly] suspicious that [the] OIP server is not under SDL.”³⁵⁷ Indeed, as Microsoft’s SDL explains, the type of static analysis security tests that are part of the test environment under the SDL the purpose of such a security test is to “look[] for known issues.”³⁵⁸ Therefore, if SolarWinds had performed such static

³⁵³ SW-SEC00574523–524 at 523. (“OIP client does not verify server host [...] *Description:* OIP client currently follows redirects and loads content without verifying certificates are from solarwinds.com . *Risk:* If OIP client is redirected from api.solarwinds.com to a site controlled by an attacker, it would load and use malicious content. *Who can exploit*:* Anyone who can locally redirect the client or subvert our F5 or server to redirect to a third-party site.”).

³⁵⁴ SW-SEC00000673–678 at 678. (Tomas Vrabec: “If SDL is not enforced for OIP, we should do it ASAP and consider additional actions to make sure that OIP is very well protected.”); at 677. (Paul Gray: “I don’t believe we cover OIP today with the SDL, but we should.”).

³⁵⁵ SW-SEC00000673–678 at 678. (“However during our analyses I found out that OIP server is using vulnerable library [...], there is public CVE [a Common Vulnerability and Exposure record] [...]. This raise strong suspicious [sic] that OIP server is not under SDL.”).

³⁵⁶ See OWASP, “A06:2021 – Vulnerable and Outdated Components,” 2021, https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/.

³⁵⁷ SW-SEC00000673–678 at 678. (“However during our analyses I found out that OIP server is using vulnerable library [...], there is public CVE [a Common Vulnerability and Exposure record] [...]. This raise strong suspicious [sic] that OIP server is not under SDL.”).

³⁵⁸ Microsoft, “Perform Security Testing,” <https://www.microsoft.com/en-us/securityengineering/sdl/practices/security-testing> (“Implement Static Analysis Security testing (SAST) - Analyzing the source code prior to compilation provides a highly scalable method of security code review and helps

analysis security tests while developing OIP, SolarWinds might well have discovered the use of a publicly available vulnerable library, and either prevented the OIP server from using it, or put in mitigations to compensate for the vulnerability. Given that these security tests are “typically integrated into the developer workflow identifying simple to detect issues *before* code is committed and into build automation [emphasis added],”³⁵⁹ if OIP had been built using SDL, any reliance on publicly known vulnerable libraries likely would have been caught and remediated before deployment.

178. Similarly, an internal assessment on July 30, 2020 found that the “OIP server may be vulnerable to SQL Injection.”³⁶⁰ SQL injection is a type of cyber-attack where an attacker inserts malicious SQL code into an input field of a database application, exploiting vulnerabilities in the application’s database query handling. This allows the attacker to manipulate the database, gaining unauthorized access to sensitive data such as usernames, passwords, and other personal information.³⁶¹ A successful SQL attack may also give an attacker control over the server on which the database resides.³⁶² On the bright side, the type of analyses that are a standard part of an SDL can quite often detect SQL injection vulnerabilities before the software is deployed, giving organization a chance to remediate the issue.³⁶³ According to

ensure that secure coding policies are being followed. It looks for known issues based on the application’s logic and adherence to coding standards, rather than when the application is running.”)

³⁵⁹ Microsoft, “Perform Security Testing,” <https://www.microsoft.com/en-us/securityengineering/sdl/practices/security-testing> (“SAST [Static Analysis Security testing] is typically integrated into the commit pipeline to identify vulnerabilities each time the software is built or packaged.”).

³⁶⁰ SW-SEC00456419 at tab ‘All Security Issues,’ row 1213.

³⁶¹ See, e.g., OWASP, “SQL Injection,” https://owasp.org/www-community/attacks/SQL_Injection.

³⁶² See, e.g., OWASP, “SQL Injection,” https://owasp.org/www-community/attacks/SQL_Injection.

³⁶³ OWASP, “Static Code Analysis,” available on January 25, 2020, https://web.archive.org/web/20200125043650/https://owasp.org/www-community/controls/Static_Code_Analysis. (“Static Code Analysis (also known as Source Code Analysis) is [...] carried out at the Implementation phase of a Security Development Lifecycle (SDL). [Static analysis is also great for] things that such tools can automatically find with high confidence, such as buffer overflows, SQL Injection Flaws, etc.”).

Mr. Brown, SolarWinds relied primarily upon a product called Checkmarx to complete static code analysis as a part of its SDL process,³⁶⁴ and, indeed, after deciding to bring OIP under SDL this tool detected the SQL injection vulnerability.³⁶⁵ Therefore, if OIP had been developed under SDL, it is likely that it would have avoided deploying OIP while it contained this SQL injection vulnerability.

179. The existence of another vulnerability that SolarWinds found in OIP after deciding to bring OIP under SDL indicates serious issues with SolarWinds' software development process. An internal document from September 2020 stated the following:³⁶⁶

Description: *OIP business layer plugin is running as a SYSTEM*

and executes tasks from 'C:\ProgramData\SolarWinds

Orionimprovement\Config' which can be written by low privilege

users (IUSR or NetworkService).

Risk: *Local privilege escalation, malicious code execution*

Who can exploit: *Local low privilege account. [...]*

Fix: *Set proper write permissions or implemented tamper*

³⁶⁴ Brown Deposition at 198:15-20 (“A. Because we’ve implemented new technology under that program. So we’ve, uh, acquired a product called Checkmarx that we expect to be run on every program, every product. We’ve acquired a product called Whitesource that does OpenSource scanning. So we expect that to be deployed everywhere.”); at 240:5-7 (“A. Uh, code analysis could be Checkmarx, Whitesource. It could -- could be implementing tools across the platform.”).

³⁶⁵ SW-SEC00273121–188 at 123 (“CheckMarx found possible SQL Injection vulnerabilities in OIP Server. [...] Who can exploit: Anyone, OIP endpoint is not authenticated.”); at 133 (“OIP client currently runs any SQL statement or SWIS query, retrieves any registry value or file. Risk: If OIP configuration is compromised, attackers could modify the database, retrieve sensitive data from the db [database] / registry / file system. Who can exploit. Anyone with access to the configuration files at rest [...] This may enable a Second-Order SQL Injection attack [CheckMarx URL][.] This vulnerability is in DatabaseHelper and SqlUserAccountProcessor classes.”).

³⁶⁶ SW-SEC00273121–188 at 136.

protection.

CVSS: 7.6

180. What the description quoted above makes clear is that OIP, as shipped, included a vulnerability that caused the security of the system to rely on the contents of a file that could be overwritten by *any user* on the system. Therefore, a malicious user could overwrite legitimate content of the file with malicious content and effectively take control of the system when the OIP software proceeded to make use of the altered file. In my book published in 2003, I warned programmers against this very issue by cautioning: “Don’t use world-writable storage [i.e., any user with low privilege can write to it], even temporarily” and “Don’t trust user-writable storage not to be tampered with.”³⁶⁷ As I explained in this book: “The reason that this is so crucial is that would-be attackers can and will examine every aspect of your software for flaws; storing important information in a world-writable storage area gives them an opportunity to compromise the security of your code, by reading or even altering the data that you store.”³⁶⁸

181. If SolarWinds had been subjecting OIP to an SDL, SolarWinds would have caught this at the design phase because this is the type of thing that a threat model and a design review is supposed to look for. If the tests during the design phase didn’t uncover this problem, it’s possible that the testing done during the implementation phase might have found the problem. If the problem wasn’t turned up in the implementation phase either, it might have been found during testing prior to deployment. Put simply, if SolarWinds had subjected OIP to a “secure development lifecycle [that] follows standard security practices”—as the Security

³⁶⁷ Graff and Van Wyk (2003) *Secure Coding: Principles and Practices*, p. 121.

³⁶⁸ Graff and Van Wyk (2003) *Secure Coding: Principles and Practices*, p. 121.

Statement asserted,³⁶⁹ then such a fundamental and serious security vulnerability likely would have been detected and remediated prior to deployment.

182. Additionally, not only does the existence of this vulnerability show that the Security Statement’s assertions regarding SDL were not followed, but also, by failing to subject OIP to these methods, reviews, and tests—and, therefore, deploying OIP with the vulnerability described above—SolarWinds also violated the following assertion of the Security Statement: “[a]ccess controls to sensitive data in our databases, systems, and environments are set on a need-to-know / least privilege necessary basis,”³⁷⁰ because anyone had “write” access (*i.e.*, anyone could modify the contents of the file). This is also clear from the fact that the “fix” that the internal document identified for this issue was to “*Set proper write permissions or implemented tamper protection*”—which are access control related remediations.³⁷¹

183. In my opinion and experience, the sections of the Security Statement that relate to SDL suggest that all software that SolarWinds developed was under security best practices.³⁷² In fact, as a cybersecurity professional, it makes no sense to me that SolarWinds would apply security best practices to their products but leave vulnerable the internal applications used to run their business, and I do not interpret the assertions in the Security Statement in that way. This is especially true with respect to applications that, while technically not products, were nevertheless

³⁶⁹ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132. (“Our secure development lifecycle follows standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments.”).

³⁷⁰ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132.

³⁷¹ SW-SEC00273121–188 at 136. Emphasis added.

³⁷² SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132. (“We follow a defined methodology for developing secure software designed to increase resiliency and security of our products. Security and security testing are implemented throughout the **entire** software development methodology. Quality Assurance is involved at each phase of the lifecycle and security best practices are a mandated aspect of **all** development activities.” Emphasis added.).

intended to be used by SolarWinds’ customers, such as OIP. The fact that, contrary to what the Security Statement appears to suggest, SolarWinds did not apply the SDL to the entire software development process, also meant that it was not able to detect risks promptly in other areas discussed in the Security Statement, such as access control. Because this is true, the Security Statement’s categorical statements about, for example, access control and least privilege, are directly called into question.

c. Internal documents contradicted the assertion that SolarWinds’ secure development lifecycle follows standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments

184. In contradiction with the public statement that SolarWinds’ “secure development lifecycle follows standard security practices including vulnerability testing, regression testing, penetration testing, and product security assessments,”³⁷³ SolarWinds’ internal communications show that some “standard security practices” were not followed consistently or, in some cases, were entirely absent.

185. For example, in a May 21, 2018 email sent to Mr. Brown and SolarWinds’ CIO Rani Johnson, Mr. Colquitt (SolarWinds’ Director of Software Development) stated that “[Threat Modeling] is a process. It’s part of the SDL and we are just barely beginning to understand how teams are going to be doing this activity.”³⁷⁴ As I described above, both OWASP and Microsoft asserted during the Relevant Period that threat modeling is an important

³⁷³ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132.

³⁷⁴ SW-SEC00237608–609 at 608.

part of designing secure software.³⁷⁵ As I described in my book “Secure Coding – Principles & Practices,” threat modeling is “the process of examining who is likely to attack a system and how they are likely to attack it.”³⁷⁶ Undertaking a threat analysis is advisable because, among other things, it “help[s] during the design and implementation of the application by guiding the designer on what defenses to put in place to protect the application.”³⁷⁷ Threat modeling in an SDL provides development teams with a structured framework that organization use to identify, evaluate, and document the security implications of their design even before they start implementation.³⁷⁸ When Mr. Colquitt stated on May 21, 2018 that “we are just barely beginning to understand how teams are going to be doing this activity,”³⁷⁹ the Security Statement had already been publicly available on SolarWinds’ website for at least six months.³⁸⁰

186. This lack of threat modeling persisted into July 2019, when an internal security evaluation of three key MSP products (“RMM,” “NCentral,” and “Backup”) found that “[n]o

³⁷⁵ See e.g., OWASP, “OWASP in SDLC,” *available on* October 20, 2020, https://web.archive.org/web/20201020193959/https://owasp.org/www-project-integration-standards/writeups/owasp_in_sdgc/. See also, Microsoft, “What Are the Microsoft SDL Practices?,” *available on* January 09, 2019, <https://web.archive.org/web/20190109013652/https://www.microsoft.com/en-us/securityengineering/sdl/practices>.

³⁷⁶ Graff and Van Wyk (2003) *Secure Coding: Principles and Practices*, p. 144.

³⁷⁷ Graff and Van Wyk (2003) *Secure Coding: Principles and Practices*, p. 144.

³⁷⁸ See Microsoft, “What Are the Microsoft SDL Practices?,” *available on* January 09, 2019, <https://web.archive.org/web/20190109013652/https://www.microsoft.com/en-us/securityengineering/sdl/practices>.

³⁷⁹ SW-SEC00237608–609 at 608.

³⁸⁰ In contradiction to his statement in the email quoted above, in his deposition, Mr. Colquitt said that “Threat modeling [...] was already happening” at the time when he sent this email. I find his statement in the email to be unambiguous and definitive with regard to the lack of threat modeling, as a consistent process, at that time. Colquitt Deposition at 142:18-19. Consistent with this, at most, what I have seen from around this time that may relate to threat modeling, was an internal document from March 5, 2018, which shows a diagram labelled “Threat Model” with the sub-title “High level thread [sic] model.” From a cybersecurity perspective, this diagram certainly does not constitute, in my opinion, a threat model. (See, e.g., Conklin, Larry, “Threat Modeling Process,” OWASP, https://owasp.org/www-community/Threat_Modeling_Process#data-flow-diagramsdata-flow-diagrams.) If SolarWinds intended this to eventually become a threat model, then this diagram was consistent with Mr. Colquitt’s May 2018 email that SolarWinds was “just barely beginning to understand how teams are going to be doing” threat modeling. SW-SEC-SDNY_00055027.

threat modelling [sic] nor analysis is performed as part of any process (except MSP Backup Engineering).”³⁸¹ This severely problematic finding contradicts the Security Statement’s assertion that “security best practices are a mandated aspect of all development activities.”³⁸² Additionally, as I described in **Section IV.B**, SolarWinds found a “significant insider threat” that SolarWinds posed to its MSP customers.³⁸³ One of the most important aspects of threat modeling is to consider the insider threat—that is malicious actions that might be taken by trusted insiders such as employees.³⁸⁴ In threat modeling, we would also consider a related analysis, which is what an attacker could accomplish by gaining control of an employee’s credentials so that they can impersonate the employee.

187. If SolarWinds had performed threat modeling on its MSP products, SolarWinds likely would have identified and fixed this insider threat issue before deploying the flawed software to customers.³⁸⁵

188. Finally, Mr. Brown testified that penetration testing may not have been “done a hundred percent of the time.”³⁸⁶ Further on this point, Harry Griffiths testified that there were

³⁸¹ SW-SEC00166790–799 (MSP Products Security Evaluation, July 2019) at 794.

³⁸² SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132.

³⁸³ SW-SEC00631418–427 (Presentation, “MSP Support Security Improvement,” November 2019) at 419.

³⁸⁴ CISA, “Defining Insider Threats,” <https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats>. (“Insider threat is the potential for an insider to use their authorized access or understanding of an organization to harm that organization. An insider is any person who has or had authorized access to or knowledge of an organization’s resources, including personnel, facilities, information, equipment, networks, and systems.”).

³⁸⁵ SW-SEC00631418–427 (Presentation, “MSP Support Security Improvement,” November 2019) at 419. Emphasis omitted from original. (“MSP Support staff has a significant level of **system level access** to both MSPs and MSP customers. The level of access is **excessive** and if abused **poses a significant insider threat**. Currently, a support person has the ability to gain privileged access, connect or run procedures on one or more MSPs and their customer environments.” Emphasis added.).

³⁸⁶ Brown Deposition at 134:10-22. (“Q. At the time that the security statement was posted at SolarWinds’ website were you aware of any instances where penetration [testing] was not done as part of the software development lifecycle? [...] A. So I cannot guarantee that it was done everywhere. I didn’t do an exhaustive audit of everywhere,

many instances in 2019 in which customers often conducted their own penetration testing and found vulnerabilities that SolarWinds had not caught internally.³⁸⁷ In my opinion, if customers often found vulnerabilities that SolarWinds had missed before releasing its products, this should have alerted SolarWinds leadership that its own penetration testing was not following “security best practices” as asserted in the Security Statement.³⁸⁸ “Best practices” would entail that the company modify its penetration testing methodology so that it could find and fix, prior to distributing the software to customers, the same vulnerabilities that its customers were finding in products.

d. SolarWinds’ internal SDL practices were inconsistent with its public representations in the Security Statement

189. Based on my experience in evaluating the cybersecurity practices of large organizations, my review of SolarWinds’ internal documentation, communications, and testimony, and considering the language of the SolarWinds Security Statement, I conclude that the security of SolarWinds’ software development process depicted in the company’s internal discussions did not match several of the very broad, categorical and unqualified assertions in the Security Statement.

but penetration testing was definitely done from an internal perspective and in some cases an external perspective for -- but I cannot say that it was done a hundred percent of the time.”).

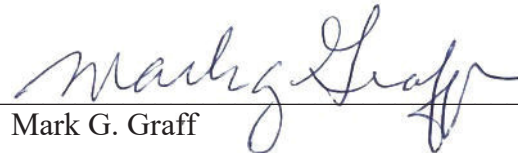
³⁸⁷ Deposition of Harry Griffiths, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, September 30, 2024 (“Deposition of Harry Griffiths”) at 42:17-51:9. (“Q. [Do] you recall any instances where customers did their own pen testing, identified a vulnerability, sent it to you, you sent it over to the engineering team for validation and they validated that there was, indeed, a vulnerability? A. Yes. [...] I can’t recall specific examples. There was a lot. There was many over the period of time. [...] they would have begun in [...] 2019 maybe. [...] Q. [Do] you recall any instances where a customer uncovered one of these vulnerabilities and people inside SolarWinds expressed concern that this is something we should have uncovered ourselves with our own pen testing? A. I don’t recall any specifics, but it’s -- it’s possible. [...] As I mentioned before, they could be using a completely different product that has, you know, patented or specific rules, scanning that only their product has [...]. As mentioned, there’s so many of these tools out there.”).

³⁸⁸ SW-SEC00466120–142 (SolarWinds’ Security Statement) at 132.

190. As noted above, no organization has perfect cybersecurity and that any organization diligently assessing its cybersecurity will uncover, from time to time, some issues needing to be addressed. However, the software development problems that I explain in this expert report, reflected in the SolarWinds internal documents and testimony, do not constitute the kind of routine minor problems that a company would encounter if it followed security best practices and industry norms in the manner described in the Security Statement. In my opinion, the discrepancies between SolarWinds' internal documents and Security Statement within the area of secure development lifecycle processes are reflective of significant deviations from industry norms, with potential company-wide impact, and in some cases an impact on the security of its customers as well.

* * *

Signed on October 25, 2024, at Fayetteville, Arkansas.



Mark G. Graff

APPENDIX A

MARK G. GRAFF

mark@telligraff.com • www.markgraff.com • @istopbadguys

CHIEF INFORMATION SECURITY OFFICER EXPERT WITNESS & CONSULTANT

Senior executive with decades of success in cyber security, application security, national security, and broadcasting. Strategic problem solver with the ability to remain calm in critical situations. Broad range of specialty fields including information security, risk assessment and management, election security, team building and development, security awareness and training, software development, and software security. Author of several books including the seminal “Secure Coding” (2003). Host of radio show/podcast, “Cyber Matters with Mark Graff” (2015-2022).

CRITICAL LEADERSHIP INITIATIVES

- Expert witness for major federal agency on groundbreaking litigation (2023-2024).
- Adjunct professor for University of Arkansas at Little Rock lecturing on cybersecurity (2023-2024).
- Shared cyber security responsibility for protecting America’s nuclear secrets over a nine-year period, successfully upholding all security measures, combating attempted breaches, and negotiating with multiple federal regulators.
- Worked with state governments (2018-2019) to identify and address election security risks.
- Expert witness in application security for the Federal Trade Commission in router/firewall litigation (2017-2019).
- Protected NASDAQ OMX, the largest stock market company in the world, from cyberattack, as CISO (2012-2015).
- Founded cybersecurity collaboration group for World Federation of Exchanges.
- Developed and hosted the first-ever gathering of world stock market security experts, the Defense of International Markets & Exchanges Symposium, in April 2014.
- Established first-ever radio show focusing on bringing cyber security to the general public.
- Expert witness for California on electronic voting system software (2008-2009) and U.S. Congress (2000, 2012).
- Co-founder of Para-Protect Services, a startup company that was first to make a profit from managed security services.

CAREER TRACK

CEO & Founder, TELLAGRAFF LLC 2015 to Present

- Established cyber security consulting firm to deliver critical threat and risk evaluation and remediation, C-level and Board-level training and decision support, expert witness services, keynote addresses and presentations to technical and non-technical audiences, and technical product development guidance.
- Authored chapter on authentication for authoritative cyber security manual (CBK CISSP study guide), 2019
- Established strategic professional relationships/board positions with leading/emerging cyber security firms.
- Cyber expert for national news outlets and publications including CNN International, CBS News, Wall Street Journal.

Chief Information Security Officer, NASDAQ QMX 2012 to 2015

- Managed a \$17-20 million budget and led a team of 30 staff to secure worldwide operations and data against cyber-attacks by foreign countries, criminal organizations, and other hostile entities.
- Directed global security policy, awareness and training, quality in software development, risk assessments, and application security.
- Created and hosted the first-ever gathering of Information Security Experts from global exchanges and stock markets, the Defense of International Markets & Exchanges Symposium (April 2014).

Chief Cyber Security Strategist, LAWRENCE LIVERMORE NATIONAL LAB 2008 to 2012

- Designed and wrote complex software utility for DOE sites to detect Personally Identifiable Information and other sensitive data on workstations and servers.
- Conducted numerous cyber security research projects and risk analyses, including classified systems.
- Key advisor to senior executive team on cyber policy, strategy, R&D topics, and potential investments.

Chief Cyber Security Officer, LAWRENCE LIVERMORE NATIONAL LAB 2003 to 2008

- Led comprehensive Cyber Security Program across unclassified and classified operations, overseeing a \$23 million budget and 60 employees, including teams for incident response, security training and awareness, and internal audits.
- Oversaw regulatory compliance with DOE and NNSA standards, while managing the policy and procedure formulation for internal projects.
- Negotiated compliance schedules and contractual agreements with federal regulatory officials and agencies.

- Spearheaded laboratory-wide FISMA-mandated certification and accreditation program, implementing a Safe Harbor approach to move lab forward while meeting rigid compliance requirements.

Vice President & Chief Scientist, PARA-PROTECT

2000 to 2002

- Managed technology forecasting, security trend and threat analysis, and led promotional activities to raise awareness of necessity of secure future for global information infrastructure.
- Assisted in the development and execution of managed security service portfolio, including incident prevention and response.

Manager, Information Security Deployment, SUN MICROSYSTEMS

1992 to 2000

- Held a range of increasingly responsible positions from Security Coordinator (1993-1997) to Network Security Architect (1997-1999) to Manager, Information Security Deployment (1999-2000)
- Responsible for corporate global programs to measure security risks and deploy countermeasures, including program and resource development, security awareness training, and lecturing.
- Testified before U.S. Congress, delivered invited lectures to nuclear research laboratories and the American Academy for the Advancement of Science on information security measurement and risk assessment techniques.

EDUCATION

UNIVERSITY OF SOUTHERN MISSISSIPPI
BS, COMPUTER SCIENCE, 1978

CERTIFICATION & TRAINING

CISSP CERTIFICATION (2017, 2009)
FCC AMATEUR EXTRA BROADCAST LICENSE (2009)
1000+ HOURS OF COMMERCIAL TRAINING
3000+ HOURS OF TECHNICAL TRAINING

MILITARY EXPERIENCE

U.S. AIR FORCE
COMPUTER TECHNICIAN, 1975-1979

BOARDS & ADVISORY ROLES
TECHNICAL ADVISORY BOARD MEMBER

FORUM OF INCIDENT RESPONSE & SECURITY TEAMS
(FIRST)

FORMER CHAIR

LA HONDA-PESCADERO UNIFIED SCHOOL DISTRICT
FORMER PRESIDENT & BOARD MEMBER

HONORS & AWARDS

INFORMATION SECURITY EXECUTIVE OF THE YEAR FOR NORTHEAST US, 2014

“KEEP IT SAFE” EDUCATIONAL VIDEO - TELLY AWARD, 2000

TESTIFIED BEFORE CONGRESS 2000, 2012

SELECTED PUBLICATIONS

OFFICIAL (ISC)2 GUIDE TO THE CISSP CBK
Co-AUTHOR, 2019
ENTERPRISE SOFTWARE SECURITY, ADDISON-WESLEY
Co-AUTHOR, 2014
E-VOTING AND FORENSICS: PRYING OPEN THE BLACK BOX
Co-AUTHOR, 2009
SECURE CODING, O'REILLY ASSOCIATES
Co-AUTHOR, 2003
TWENTY YEARS OF INTERNET SECURITY, NEXT TWENTY YEARS NEWSLETTER
AUTHOR, 2001
PEXLIB: A REFERENCE MANUAL, PRENTICE-HALL
AUTHOR, 1994
THE ACCESS CONTROL EXECUTIVE: PSYCHOLOGICAL ELEMENTS OF COMPUTER SECURITY, MONOGRAPH
AUTHOR, 1987

SELECTED FEATURES AND OPINION PIECES

INC., FORBES, USA TODAY, SF CHRONICLE, CSO
MAGAZINE, PC MAGAZINE, CNN INTERNATIONAL, CBS
RADIO, THE INTERCEPT

SELECTED SPEAKING ENGAGEMENTS

“CYBER MATTERS WITH MARK GRAFF”
RADIO SHOW HOST
NYIT CYBER SECURITY CONFERENCE (2016)
KEYNOTE SPEAKER
ACM CPR SIG (2015)
KEYNOTE SPEAKER
SPLUNK CYBER SECURITY CONFERENCE (2014)
KEYNOTE SPEAKER

APPENDIX B

Prior Testimony

1. Federal Trade Commission v. D-Link Systems, Inc., *3:17-Cv-00039-JD*, United States District Court, Northern District of California. Report (2016) and Deposition (2018).
2. Epic Games, Inc., v. Apple Inc., *4:20-CV-05640-YGR*, United States District Court, Northern District of California. Declaration (2020).

APPENDIX C

Materials Considered

Legal Documents

Amended Complaint, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, February 16, 2024.

Complaint, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, October 30, 2023.

Declaration of Serrin Turner in Support of Defendants' Motion to Dismiss Amended Complaint, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, December 17, 2020.

Memorandum of Law in Support of Defendants' Motion to Dismiss the Amended Complaint, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, March 22, 2024.

Motion to Dismiss the Amended Complaint, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, March 22, 2024.

SolarWinds Corp.'s Responses and Objections to Plaintiff's First Requests for Admission to Defendant SolarWinds Corp, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, May 17, 2024.

Supplemental Wells Submission on Behalf of SolarWinds Corporation, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, December 23, 2022.

Wells Submission on Behalf of J. Barton Kalsu, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, June 30, 2023.

Wells Submission on Behalf of Kevin Thompson, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, June 30, 2023.

Wells Submission on Behalf of Rani Johnson, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, June 12, 2023.

Wells Submission on Behalf of SolarWinds Corporation, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, November 22, 2022.

Wells Submission on Behalf of Timothy Brown, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, June 30, 2023.

Wells Submission on Behalf of Woong Joseph Kim, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, June 16, 2023.

Depositions and Investigative Testimony

Deposition of Brad Cline and associated exhibits, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, October 1, 2024.

Deposition of Brent Thill and associated exhibits, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, August 28, 2024.

Deposition of Eric Quitugua and associated exhibits, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, September 17, 2024.

Deposition of Harry Griffiths and associated exhibits, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, September 30, 2024.

Deposition of Ian Edward Thornton-Trump and associated exhibits, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, October 18, 2024.

Deposition of Jason Bliss (30(b)(6)) and associated exhibits, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, October 16, 2024.

Deposition of Kellie Jaie Pierce and associated exhibits, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, July 24, 2024.

Deposition of Kevin Thompson and associated exhibits, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, October 2, 2024.

Deposition of Matthew Hedberg and associated exhibits, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, July 26, 2024.

Deposition of Rani Johnson and associated exhibits, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, August 27, 2024.

Deposition of Steven Colquitt and associated exhibits, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, September 18, 2024.

Deposition of Timothy Brown and associated exhibits, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, October 3, 2024.

Deposition of Woong Joseph Kim and associated exhibits, *Securities and Exchange Commission v. SolarWinds Corp. and Timothy G. Brown*, 23-cv-09518-PAE, September 16, 2024.

Investigative Testimony of Brad Cline and associated exhibits - Vol. I, August 17, 2021.

Investigative Testimony of Danielle Campbell and associated exhibits - Vol. I, October 18, 2021.

Investigative Testimony of Eric Quitugua and associated exhibits - Vol. I, August 31, 2021.

Investigative Testimony of Eric Quitugua and associated exhibits - Vol. II, September 1, 2021.

Investigative Testimony of Eric Quitugua and associated exhibits - Vol. III, July 15, 2022.

Investigative Testimony of Harry Griffiths and associated exhibits - Vol. I, June 21, 2022.

Investigative Testimony of Harry Griffiths and associated exhibits - Vol. II, June 22, 2022.

Investigative Testimony of Kellie Jaie Pierce and associated exhibits - Vol. I, October 27, 2021.

Investigative Testimony of Kellie Jaie Pierce and associated exhibits - Vol. II, October 28, 2021.

Investigative Testimony of Kevin Thompson and associated exhibits - Vol. I, September 1, 2022.

Investigative Testimony of Rani Johnson and associated exhibits - Vol. I Part 1, February 10, 2022.

Investigative Testimony of Rani Johnson and associated exhibits - Vol. I Amended, March 17, 2022.

Investigative Testimony of Timothy Brown and associated exhibits - Vol. I, March 8, 2022.

Investigative Testimony of Timothy Brown and associated exhibits - Vol. II, March 9, 2022.

Investigative Testimony of Timothy Brown and associated exhibits - Vol. III, June 15, 2022.

Investigative Testimony of Woong Joseph Kim and associated exhibits - Vol. I, October 3, 2022.

Bates-Stamped Documents Cited

SW-SEC00000673–678.
 SW-SEC00001464.
 SW-SEC00001476–484.
 SW-SEC00001497–550.
 SW-SEC00010210–229.

SW-SEC00012265–275.
SW-SEC00024906–914.
SW-SEC00043080–084.
SW-SEC00043620–630.
SW-SEC00045356–357.
SW-SEC00045358.
SW-SEC00151415–421.
SW-SEC00166790–799.
SW-SEC00168009–017.
SW-SEC00168778–779.
SW-SEC00168780.
SW-SEC00223527–532.
SW-SEC00237608–609.
SW-SEC00254254–266.
SW-SEC00273121–188.
SW-SEC00292763–781.
SW-SEC00298504.
SW-SEC00298504–519.
SW-SEC00336293–294.
SW-SEC00337101–109.
SW-SEC00356992–7083.
SW-SEC00386134–143.
SW-SEC00407702–707.
SW-SEC00427486–488.
SW-SEC00456419.
SW-SEC00459171–305.
SW-SEC00466120–142.
SW-SEC00574523–524.
SW-SEC00578414–476.
SW-SEC00631418–427.
SW-SEC00632171–200.
SW-SEC-SDNY_00050922.
SW-SEC-SDNY_00055027.

Bates-Stamped Documents Considered

CPIB-SEC-SW-00000000–00000029.
FEYE_SEC_0000000000–0000000211.
HOLTZMAN_0000001–0013568.
KALSU_0000001–0000029.
KPMG-Solar Winds-WP-0000001–0002511.
LURIE0000001–0010959.
MAN_SEC000212–000219.
MLR_000001–008967.
MSFT-SEC-SW-0000000–0000045.
MSFT-SEC-SW-0000056–0005549.
NETSKOPE_000001–000079.

PAN-00000007-00000447.
 PWC-SEC-00000001-00047013.
 PWC-SEC-00047017-00047488.
 SEC-AMAZON-E-000000001.
 SEC-CORR-E-00000001-0000189.
 SEC-HOLTZMAN-E-00000001-0000002.
 SEC-IB-E-000000001-000009626.
 SEC-KalsuJ-E-00000001-0000004.
 SEC-KimJ-E-00000001-0000010.
 SEC-KPMG-E-00000001-0000004.
 SEC-MANDIANT-E-00000001-0000002.
 SEC-MICROSOFT-E-000000000-000000050.
 SEC-MLPFS-E-000000000-000000103.
 SEC-MLR-E-00000001-0000004.
 SEC-NETSKOPE-E-00000001-0000015.
 SEC-PWC-E-000000001-000000050.
 SEC-SCHWAB-E-000000001-000001424.
 SEC-SEC-E-00000001-0000526.
 SEC-SW-E-00000001-0000105.
 SEC-ThompsonK-E-00000001-0000016.
 SILVER_LAKE_PRIVILEGE_LOG_000000001-000000032.
 SL-SEC-00000001-00003086.
 SOLARWINDS_PRIV_LOG-00000001-0000003.
 SWI-000000499-000000512.
 SW-RJ-SEC00000001-00000538.
 SW-SEC00000000-00000293.
 SW-SEC00000297-00391127.
 SW-SEC00391138-00647807.
 SW-SEC00647855-00666851.
 SW-SEC-SDNY_00000001-00046825.
 SW-SEC-SDNY_00050461.
 SW-SEC-SDNY_00050922.
 SW-SEC-SDNY_00050927-00050928.
 SW-SEC-SDNY_00051902.
 SW-SEC-SDNY_00052137.
 SW-SEC-SDNY_00052226.
 SW-SEC-SDNY_00053415.
 SW-SEC-SDNY_00053536.
 SW-SEC-SDNY_00053939-00053940.
 SW-SEC-SDNY_00055027.
 SW-SEC-SDNY_00055107-00055108.
 SW-SEC-SDNY_00055111-00055112.
 SW-SEC-SDNY_00055205-00055208.
 TB-SEC-00000001-00014504.
 THOMPSON_SEC00000001-00001702.

Books

- Graff, Mark G., and Kenneth R. Van Wyk, "Secure Coding: Principles and Practices," O'Reilly Media, June 30, 2003.
- Humble, Jez, and David Farley, *Continuous Delivery*, Pearson Education, 2011.
- John, Warsinske, Mark Graff, Kevin Henry, *et al.*, "Chapter 5 - Identity and Access Management," *The Official (ISC) Guide to the CISSP CBK Reference*, 5th Ed., Wiley, April 2019.
- Van Wyk, Kenneth R., Mark G. Graff, Dan S. Peters, *et al.*, *Enterprise Software Security: A Confluence of Disciplines*, Addison Wesley Professional, December 7, 2014.

Public Documents

- Article 32 of the General Data Protection Regulation (GDPR): Security of Processing. Sarbanes-Oxley Act of 2002.*
- SolarWinds Corporation, SEC Form 10-K, filed December 31, 2020.
- SolarWinds Corporation, SEC Form S-1, filed October 18, 2018.
- Adobe, "The Adobe Secure Product Lifecycle (SPLC)," <https://www.adobe.com/trust/security/adobe-splc.html>, accessed October 22, 2024.
- Assis, Claudia, "Software Provider SolarWinds Files for IPO," *MarketWatch*, September 21, 2018, <https://www.marketwatch.com/story/software-provider-solarwinds-files-for-ipo-2018-09-21>, accessed September 20, 2024.
- Baker, Liana B., and Greg Roumeliotis, "SolarWinds Confirms It Is Exploring Strategic Alternatives," *Reuters*, October 9, 2015, <https://www.reuters.com/article/us-solarwinds-m-a/exclusive-solarwinds-in-talks-with-buyout-firms-about-a-sale-sources-idUSKCN0S31OT20151009>, accessed September 20, 2024.
- Brown, Timothy, "Do Your Vendors Take Security Seriously?," *N-able Technologies*, September 10, 2020, <https://www.n-able.com/blog/do-your-vendors-take-security-seriously>, accessed September 7, 2023.
- Cimpanu, Catalin, "SEC Filings: Solarwinds Says 18,000 Customers Were Impacted by Recent Hack," *ZDNET*, December 14, 2020, <https://www.zdnet.com/article/sec-filings-solarwinds-says-18000-customers-are-impacted-by-recent-hack/>, accessed September 20, 2024.
- CIS, "The 20 CIS Controls & Resources," *available on* June 19, 2019, <https://web.archive.org/web/20190619213638/https://www.cisecurity.org/controls/cis-controls-list/>, accessed October 16, 2024.
- CISA, "About CISA," <https://www.cisa.gov/about>, accessed October 14, 2024.
- CISA, *Capacity Enhancement Guide: Implementing Strong Authentication*, October 8, 2020.
- CISA, "Defining Insider Threats," <https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats>, accessed September 20, 2024.
- CISA, "Protecting Against Cyber Threats to Managed Service Providers and their Customers," May 11, 2022, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-131a>, accessed October 20, 2024.
- CISA, "Technical Approaches to Uncovering and Remediating Malicious Activity," September 24, 2020, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-245a>, accessed September 20, 2024.

- CISA, “What is Cybersecurity?,” February 01, 2021, <https://www.cisa.gov/news-events/news/what-cybersecurity>, accessed September 20, 2024.
- CISCO, “Trustworthy Solutions,” <https://www.cisco.com/c/en/us/about/trust-center/technology-built-in-security.html#~trustworthysolutionsfeatures>, accessed October 22, 2024.
- CISCO, “What Is a CISO?,” <https://www.cisco.com/c/en/us/products/security/what-is-ciso.html>, accessed September 20, 2024.
- CISPA, *Development of Secure Software with Security by Design*, July 2014.
- Conklin, Larry, “Threat Modeling Process,” *OWASP*, https://owasp.org/www-community/Threat_Modeling_Process#data-flow-diagrams, accessed October 25, 2024.
- CWE, “CWE-256: Unprotected Storage of Credentials,” *available on* December 20, 2020, <http://web.archive.org/web/20201220094745/https://cwe.mitre.org/data/definitions/256.html>, accessed October 15, 2024.
- CWE, “CWE-798: Use of Hard-coded Credentials,” *available on* October 21, 2019, <https://web.archive.org/web/20191021162254/https://cwe.mitre.org/data/definitions/798.html>, accessed October 16, 2024.
- Evans, Woody, “3 Ways to Mitigate the Growing Risk of Non-Production Environment Breaches,” *Delphix*, March 28, 2023, <https://www.delphix.com/blog/3-ways-to-mitigate-the-growing-risk-of-non-production-environment-breaches>, accessed October 23, 2024.
- First, “Common Vulnerability Scoring System SIG,” <https://www.first.org/cvss/>, accessed October 14, 2024.
- ISO, “Information Security,” <https://www.iso.org/sectors/it-technologies/information-security>, accessed October 2, 2024.
- ISO, “ISO/IEC 27000 Family,” <https://www.iso.org/standard/iso-iec-27000-family>, accessed October 8, 2024.
- ISO, *ISO/IEC 27001:2013(E): Information Technology — Security Techniques — Information Security Management Systems — Requirements*, October 01, 2013.
- ISO, *ISO/IEC 27001:2022: Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements*, October 2022.
- Johnson, Eric, “Secure Software Development Lifecycle Overview,” *SANS*, April 7, 2015, <https://www.sans.org/blog/secure-software-development-lifecycle-overview>, accessed October 11, 2024.
- Johnson, O’Ryan, “SolarWinds Security Exec Timothy Brown: MSPs ‘Top Of My Risk Level’,” *CRN*, *available on* September 06, 2019, <https://web.archive.org/web/20210126084205/https://www.crn.com/solarwinds-security-exec-timothy-brown-msps-top-of-my-risk-level-/2>, accessed September 20, 2024.
- Johnson, Tony, “New and Improved SolarWinds Platform, Who Dis?,” *THWACK*, April 20, 2022, <https://thwack.solarwinds.com/products/the-solarwinds-platform/b/news/posts/new-and-improved-solarwinds-platform-who-dis>, accessed September 20, 2024.
- Kumbakara, Narayanan, “Managed IT Services: The Role of IT Standards,” *Information Management & Computer Security*, Vol. 16, No. 4, July 22, 2008, pp. 336–359.
- Microsoft, “About Microsoft SDL,” *available on* June 11, 2020, <https://web.archive.org/web/20200611020126/https://www.microsoft.com/en-us/securityengineering/sdl/about>, accessed October 22, 2024.
- Microsoft, “Perform Security Testing,” <https://www.microsoft.com/en-us/securityengineering/sdl/practices/security-testing>.

- Microsoft, "What Are the Microsoft SDL Practices?," *available on* January 09, 2019, <https://web.archive.org/web/20190109013652/https://www.microsoft.com/en-us/securityengineering/sdl/practices>, accessed October 02, 2024.
- Miller, Sarah, "Separation of Duties and Least Privilege (Part 15 of 20: CERT Best Practices to Mitigate Insider Threats Series)," *SEI*, July 26, 2017 <https://insights.sei.cmu.edu/blog/separation-of-duties-and-least-privilege-part-15-of-20-cert-best-practices-to-mitigate-insider-threats-series/>, accessed October 10, 2024.
- MIT, "Multics," <https://web.mit.edu/multics-history/>, accessed October 20, 2024.
- Mucci, Tim, "What Is Structured Query Language (SQL)?," *IBM*, May 31, 2024, <https://www.ibm.com/think/topics/structured-query-language>, accessed October 20, 2024.
- NIST, "Access Control Policy Testing," *available on* October 18, 2019, <https://web.archive.org/web/20191018185137/https://csrc.nist.gov/projects/access-control-policy-tool>, accessed September 20, 2024.
- NIST, "Cybersecurity," <https://www.nist.gov/cybersecurity>, accessed September 20, 2024.
- NIST, *The Economic Impacts of Inadequate Infrastructure for Software Testing*, May 2002.
- NIST, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, April 16, 2018.
- NIST, "Glossary – 'Penetration Testing'," *available on* October 19, 2020, https://web.archive.org/web/20201019101437/https://csrc.nist.gov/glossary/term/penetration_testing, accessed October 19, 2024.
- NIST, "Glossary – 'Worm'," *available on* August 13, 2020, <https://web.archive.org/web/20200813182531/https://csrc.nist.gov/glossary/term/worm>, accessed October 19, 2024.
- NIST, "Glossary – 'Access Control'," https://csrc.nist.gov/glossary/term/access_control, accessed October 23, 2024.
- NIST, "Glossary – 'Defense-in-Depth'," https://csrc.nist.gov/glossary/term/defense_in_depth, accessed September 20, 2024.
- NIST, "Glossary – 'Least Privilege'," https://csrc.nist.gov/glossary/term/least_privilege, accessed September 20, 2024.
- NIST, "Glossary – 'Separation of Duty (SOD)'," https://csrc.nist.gov/glossary/term/separation_of_duty, accessed September 20, 2024.
- NIST, *NIST Special Publication 800-37: Risk Management Framework for Information Systems and Organizations*, NIST, December 2018.
- NIST, *NIST Special Publication 800-53 Revision 5: Control Catalog Spreadsheet*, January 26, 2021, <https://csrc.nist.gov/News/2021/control-catalog-and-baselines-as-spreadsheets>.
- NIST, *NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations*, September 2020.
- NIST, *NIST Special Publication 800-63B: Digital Identity Guidelines*, June 2017.
- NIST, *NIST Special Publication 1800-11A: Data Integrity, Recovering from Ransomware and Other Destructive Events*, September 2020.
- NIST, *NIST Special Publication 1800-25: Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Event*, December 2020.
- NIST, "Role Based Access Control," June 22, 2020, <https://csrc.nist.gov/projects/role-based-access-control>, accessed October 2, 2024.

- NIST, “SQL,” *available on* October 20, 2020, <https://web.archive.org/web/20201020184906/https://csrc.nist.gov/glossary/term/SQL>, accessed October 20, 2024.
- OWASP, “A06:2021 – Vulnerable and Outdated Components,” 2021, [https://owasp.org/Top10/A06_2021-Vulnerable and Outdated Components/](https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/), accessed October 23, 2024.
- OWASP, “About the OWASP Foundation,” <https://owasp.org/about>, accessed September 20, 2024.
- OWASP, “OWASP in SDLC,” *available on* October 20, 2020, [https://web.archive.org/web/20201020193959/https://owasp.org/www-project-integration-standards/writeups/owasp in sdgc/](https://web.archive.org/web/20201020193959/https://owasp.org/www-project-integration-standards/writeups/owasp_in_sdgc/), accessed October 16, 2024.
- OWASP, “OWASP Top 10 Security Risks,” *available on* January 17, 2020, <https://web.archive.org/web/20200117090941/https://owasp.org/www-project-top-ten/>, accessed October 14, 2024.
- OWASP, “Password Plaintext Storage,” *available on* October 27, 2020, [https://web.archive.org/web/20201027103906/https://owasp.org/www-community/vulnerabilities/Password Plaintext Storage](https://web.archive.org/web/20201027103906/https://owasp.org/www-community/vulnerabilities/Password_Plaintext_Storage), accessed October 15, 2024.
- OWASP, *Secure Coding Practices: Quick Reference Guide*, November 2010.
- OWASP, “SQL Injection,” https://owasp.org/www-community/attacks/SQL_Injection, accessed October 21, 2024.
- OWASP, “Static Code Analysis,” *available on* January 25, 2020, [https://web.archive.org/web/20200125043650/https://owasp.org/www-community/controls/Static Code Analysis](https://web.archive.org/web/20200125043650/https://owasp.org/www-community/controls/Static_Code_Analysis), accessed October 19, 2024.
- OWASP, “Threat Modeling: OWASP Cheat Sheet Series,” *available on* July 16, 2019, [https://web.archive.org/web/20190716105548/https://cheatsheetseries.owasp.org/cheatsheets/Threat Modeling Cheat Sheet.html](https://web.archive.org/web/20190716105548/https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html), accessed October 19, 2024.
- PA Consulting, *GDPR - How Is Industry Addressing the Legislation*, January 25, 2017.
- Romeo, Chris, “Secure Development Lifecycle: The Essential Guide to Safe Software Pipelines,” *Security Journey*, May 3, 2019, <https://www.securityjourney.com/post/secure-development-lifecycle-the-essential-guide-to-safe-software-pipelines>, accessed October 2, 2024.
- Saltzer, Jerome H., and Michael D. Schroeder, “The Protection of Information in Computer Systems,” *Proceedings of the IEEE*, Vol. 63, No. 9, September 1975, pp. 1278–1308.
- SANS Institute, “About SANS Institute,” <https://www.sans.org/about>, accessed October 14, 2024.
- SANS Institute, *Implementing Least Privilege at Your Enterprise*, July 5, 2003.
- SANS Institute, *Inside-Out Vulnerabilities, Reverse Shells*, May 25, 2006.
- SAP, *The Secure Software Development Lifecycle at SAP*, 2020.
- Shackleford, Dave, and Arick Goomanovsky, “Mitigate Access Risk by Enforcing Least Privilege in Cloud Infrastructure,” *SANS*, September 16, 2020, <https://www.sans.org/webcasts/mitigate-access-risk-enforcing-privilege-cloud-infrastructure-116290/>, accessed October 18, 2024.
- Software Engineering Institute, “CERT Coordination Center”, <https://www.sei.cmu.edu/about/divisions/cert/index.cfm>, accessed October 14, 2014.

- SolarWinds, “Corporate Overview,” *available on* April 30, 2019, <http://web.archive.org/web/20190430082154/https://investors.solarwinds.com/overview/default.aspx>, accessed September 20, 2024.
- SolarWinds, “IT Management Software & Monitoring Tools,” *available on* April 30, 2019, <http://web.archive.org/web/20190430194414/https://www.solarwinds.com>, accessed September 20, 2024.
- SolarWinds, “Orion Improvement Program,” first published on October 15, 2018, last published on January 7, 2022, https://solarwindscore.my.site.com/SuccessCenter/s/article/Orion-Improvement-Program?language=en_US, accessed October 11, 2024.
- SolarWinds, “Orion Platform - Scalable IT Monitoring,” *available on* April 30, 2019, <http://web.archive.org/web/20190430082356/https://www.solarwinds.com/solutions/orion>, accessed September 20, 2024.
- SolarWinds, “Setting the Record Straight on the SEC and SUNBURST,” *Orange Matter*, November 8, 2023, <https://orangematter.solarwinds.com/2023/11/08/setting-the-record-straight-on-the-sec-and-sunburst/>, accessed December 1, 2023.
- SolarWinds, “SolarWinds Accelerates Its Plan for a Safer SolarWinds and Customer Community with the Appointment of Three New Executives,” May 4, 2021, <https://investors.solarwinds.com/news/news-details/2021/SolarWinds-Accelerates-its-Plan-for-a-Safer-SolarWinds-and-Customer-Community-With-the-Appointment-of-Three-New-Executives/default.aspx>, accessed September 20, 2024.
- SolarWinds, “SolarWinds Sets Its Sights on the ITSM Market through Acquisition of Samanage and Introduction of a SolarWinds Service Desk Product,” April 11, 2019, <https://investors.solarwinds.com/news/news-details/2019/SolarWinds-Sets-Its-Sights-on-the-ITSM-Market-through-Acquisition-of-Samanage-and-Introduction-of-a-SolarWinds-Service-Desk-Product/default.aspx>, accessed September 20, 2024.
- SolarWinds, “SolarWinds Transforms Brand to Signify Ongoing Evolution, Portfolio Expansion, and Customer Empowerment,” May 30, 2023, <https://investors.solarwinds.com/news/news-details/2023/SolarWinds-Transforms-Brand-to-Signify-Ongoing-Evolution-Portfolio-Expansion-and-Customer-Empowerment/default.aspx>, accessed September 20, 2024.
- SolarWinds, “SolarWinds Trust Center,” *available on* December 14, 2020, <https://web.archive.org/web/20201214181943/https://www.solarwinds.com/trust-center?promo=blog>, accessed October 2, 2024.
- SolarWinds, “Steps to Proactive Cybersecurity — SolarWinds TechPod 006,” *Orange Matter*, March 14, 2019, <https://orangematter.solarwinds.com/2019/03/14/steps-to-proactive-cybersecurity-solarwinds-techpod-006/>, accessed October 27, 2023.
- SolarWinds, “What Is FTP Server?,” <https://www.solarwinds.com/resources/it-glossary/ftp-server>, accessed October 22, 2024.
- The Department of Homeland Security, “Operational and Support Components,” <https://www.dhs.gov/operational-and-support-components>, accessed October 14, 2024.
- Thurmond, Tori, “8 Best Secure Coding Practices,” *KirkpatrickPrice*, *available on* September 27, 2020, <https://web.archive.org/web/20200927124111/https://kirkpatrickprice.com/blog/secure-coding-best-practices/>, accessed October 8, 2024.
- U.S. Department of Homeland Security, *Access Control Technologies Handbook*, September 2015.

Verizon, *2017 Data Breach Investigations Report 10th Edition*, 2017.